(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020010090014 A
(43)Date of publication of application: 18.10.2001

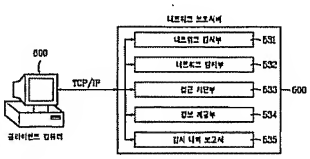
(21)Application number: 1020000024735
(22)Date of filing: 09.05.2000
(30)Priority:

(51)Int. Cl H04L 9/00

(71)Applicant: WINS TECHNET CO., LTD.
(72)Inventor: HAN, DAE SEONG
SHIN, MYEONG CHEOL

(54) SYSTEM FOR PROTECTING NETWORK

(57) Abstract:



PURPOSE: A system for protecting a network is provided to construct a more essential security organization by automatically detecting and blocking an illegal invasion such as a hacking as well as pursuing a source thereof and giving an accurate evidence of hacking. CONSTITUTION: A client computer(600) uses one operating system of a windows 95, windows 98, windows 2000 or windows NT. The client computer(600) is provided with a web browser. A network protecting server(500) uses a LINUX as an own operating system, and has a web server for providing a network protecting site therein. A network monitoring unit(531) monitors a communication in an internal/external network. A network detecting unit(532) operates in connection with the network monitoring unit(531), and automatically detects and discriminates illegal invasions. An access blocking unit(533) blocks the corresponding network session, if an internal network illegal action and an external hacking have been detected in the network detecting unit(532). An alarm generating unit(534) informs a client that the internal network illegal action and external hacking have been detected. A unit for reporting details of monitoring(535) reports details of monitoring and detecting during a certain period, and a logging.

Legal Status
Date of request for an examination (20000509)
Notification date of refusal decision (00000000)
Final disposal of an application (rejection)
Date of final disposal of an application (20020515)
Patent registration number ( )
Date of registration (00000000)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent (00000000)
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

특2001-0090014

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 9/00

(11) 공개번호 특2001-0090014
(43) 공개일자 2001년10월18일

(21) 출원번호 10-2000-0024735
(22) 출원일자 2000년05월09일

(71) 출원인 주식회사 윈스테크넷 김대연
서울특별시 강남구 삼성동 144-25
(72) 발명자 신명철
서울특별시관악구신림4동496-23
한태성
경기도남양주시퇴계원면광남리아파트104-306
(74) 대리인 심창섭, 김용인

심사청구 : 있음

(54) 네트워크 보호 시스템

요약

본 발명은 네트워크 시스템에 있어서, 특히 네트워크 연결을 갖는 대상 시스템에 대한 비인가된, 비정상적인 행위를 탐지 및 구별하고, 이에 대응하기 위한 네트워크 보호 시스템에 관한 것으로, 각각 독립된 내부 네트워크와 외부 네트워크를 최적의 경로로 상호 연결시키는 라우터와, 상기 라우터에 의해 상호 연결된 경로를 통한 통신에 대해 일차적으로 감시하고 통제하는 방화벽과, 상기 방화벽에서 허가한 통신에 대해 실시간으로 감시하면서 비인가/비정상적인 통신을 구별 탐지하고, 그 탐지 내역으로부터 해당 네트워크 세션을 선택적으로 차단하고, 그 탐지 내역을 사각적 청각적으로 보고하고, 그 탐지 내역에 대한 정보를 관리하는 네트워크 보호 서버를 포함하여 구성되는 네트워크 보호 시스템에 관한 것이다.

대표도

도5

색인어

네트워크 보호 시스템, 해킹, 크래킹, 방화벽

명세서

도면의 간단한 설명

도 1은 종래 기술에 따른 네트워크 보호 시스템의 일반적인 구성을 나타낸 도면.

도 2는 본 발명에 따른 네트워크 보호 시스템의 전체 구성을 나타낸 도면,

도 3은 본 발명의 일 실시 예에 따른 네트워크 보호 시스템의 구성을 나타낸 도면.

도 4는 본 발명에 따른 네트워크 보호 시스템의 프로토콜 구조를 나타낸 도면.

도 5는 본 발명에 따른 네트워크 보호 시스템의 네트워크 보호 서버의 내부 구성과 클라이언트 컴퓨터를 나타낸 블록도.

도 6은 본 발명에서 외부 및 내부 접근 내역을 감시하기 위한 클라이언트 컴퓨터의 화면 포맷을 나타낸 도면.

도 7은 본 발명에서 내부 네트워크를 사용한 외부 사용자의 정보를 클라이언트 컴퓨터의 화면에 나타낸 도면.

도 8은 본 발명에서 해킹 정보들과 그의 조치방법을 클라이언트 컴퓨터의 화면에 나타낸 도면.

도 9는 본 발명에서 유해정보 차단 설정과 실시간 내부 서버 접속 감시를 위한 클라이언트 컴퓨터의 화면 포맷을 나타낸 도면.

도 10은 본 발명에서 다양한 조건 검색 및 그의 결과에 따른 각종 보고서를 클라이언트 컴퓨터의 화면에 나타낸 도면.

도 11은 본 발명에 따른 네트워크 보호 시스템의 마스터 관리와, 실시간 감시 네트워크 데이터 선별 로깅 관리를 위한 클라이언트 컴퓨터의 화면을 나타낸 도면.

도 12는 본 발명의 설명을 위한 인터넷프로토콜(IP) 데이터그램의 구조를 나타낸 도면.

도 13은 본 발명의 설명을 위한 전송제어프로토콜(TCP) 세그먼트의 구조를 나타낸 도면.

도면의 주요부분에 대한 부호의 설명

500: 네트워크 보호 서버	531: 네트워크 감시부
532: 네트워크 탐지부	533: 접근 차단부
534: 경보 제공부	535: 감시내역 보관부
600: 클라이언트 컴퓨터	

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 네트워크 시스템에 관한 것으로, 특히 네트워크 연결을 갖는 대상 시스템에 대한 비인가된, 비정상적인 행위를 탐지 및 구별하고, 이에 대응하기 위한 네트워크 보호 시스템에 관한 것이다.

일반적으로 인터넷(INTERNET)은 지구상의 수천만 사람들이 여러 자원들을 공유할 수 있도록 네트워크 환경을 제공해 주고 있다.

이러한 인터넷의 범 지구적인 이용 가치에 반하여 전세계는 인터넷을 통한 해킹(hacking) 특히 크래킹(cracking) 이라는 공포 속에 놓여 있다. 정보화 사회에 진입하면서 지식과 정보력이 기업과 국가의 운명을 좌우하는 시대가 도래한 만큼 전세계의 각 국가들은 자국의 지식과 정보를 보호하고, 시스템 파괴에 대비한 보안 수단을 마련하는데 계속적인 연구 및 투자를 아끼지 않고 있다.

다시 언급하자면, 기본적으로 인터넷은 정보의 공유와 개방을 목표로 개발되었다. 따라서 인터넷은 보안의 취약성을 가진다. 이 때문에 경영전략이나 핵심기술이나 연구 프로젝트 정보나 고부가가치의 서설 등과 같은 기업의 핵심, 정부 기밀이나 국가의 경제 전략이나 국방 시설 등과 같은 국가의 핵심은 물론 작게는 금융거래 내용이나 신용카드정보나 개인신상정보 등과 같은 개인의 핵심까지도 누출 침해당할 가능성이 매우 높다.

이에 따라 종래에는 해킹(특히 크래킹)이나 스니핑(sniffing) 등, 즉 인가되지 않은 비정상적인 행위로부터 인터넷에 연결되는 시스템을 보호하기 위한 기술적, 장치적 도구를 마련하는데 많은 힘을 기울이고 있다.

시스템 보호를 위한 기술적, 장치적 도구의 필수 구현 요소들을 나열하면, 특정 보안체계를 사용하여 제3자가 인터넷을 통해 전달되는 정보 내용을 획득하지 못하도록 암호화에 의해 비밀성을 유지하는 기밀성(Confidentiality)과, 전송 정보 근원지의 정보 제공자에 대한 신원을 확인하는 인증(Authentication)과, 정보가 전송 도중에 훼손되었는지의 여부(정보가 전송 도중에 권한이 없는 방식으로 변경되었는지의 여부)를 확인하는 무결성(Integrity)과, 정보를 전송한 정보 제공자가 정보 송신 사실을 허위로 부인하는 것으로부터 정보 수신자를 보호하고 정보 수신자가 정보 수신 사실을 거짓으로 부인하는 것으로부터 정보 제공자를 보호하기 위해 그에 따른 증거를 제공하는 부인방지(Nonrepudiation)가 있다.

상기 나열된 시스템 보호를 위한 기술적 장치적 도구의 필수 구현 요소들을 실현하는데 있어서 종래에는, 전송 정보를 비정상적 불법적으로 획득한 제3자가 그 정보 내용을 해석할 수 없도록 정보를 특정키로 가공하여 전송하는 암호화기술(Encryption), 일방향 해쉬함수(hash function)를 이용하여 주어진 정보를 일정 길이의 해쉬값으로 변환하여 전송하고 수신측에서는 전송 받은 정보의 해쉬값을 구하여 무결성을 확인하는 메시지 다이제스트 기술과, 개인의 신원을 확인하는 인증 기술로써 신뢰할 수 있는 인증기관으로부터 인증서를 발급 받아 특정 서비스를 이용하려는 사용자들을 구분하는 전자인증기술과, 인증과 무결성과 부인방지를 해결하기 위해 필요한 전자서명기술 등이 있었다.

그러나, 상기 나열된 시스템 보호 도구로서도 보안이 완성되었다고 볼 수 없다. 그에 따라 종래의 네트워크 보호 시스템에는 방화벽(firewall)이라는 또다른 안전 도구를 사용하고 있으며, 그와 관련된 설명을 위해 도 1을 참조한다.

도 1은 종래 기술에 따른 네트워크 보호 시스템의 일반적인 구성을 나타낸 도면이다.

도 1을 참조하면, 종래의 시스템은 정보가 전송될 최적의 경로를 선택해 주는 라우터(router)(1)와, 내부 네트워크와 외부 네트워크 사이에서 양자간의 연결점 역할을 수행하는 방화벽(firewall)(2)과, 내부 네트워크에서 여러 전송라인을 모아서 상기 방화벽(2)을 통해 라우터(1)와 접속되는 허브(HUB)들(3,4,8,12)을 기본적으로 구비한다.

도 1에서 보인 바와 같이, 허브는 각종 서버 또는 컴퓨터들의 연결뿐만 아니라 또다른 허브와의 네트워크 연결도 가능하다, 즉 자유 링크를 갖도록 구성된 인터넷 비무장지대(Internet DMZ ; Internet DeMilitarized Zone)에서의 허브(4)는 웹 환경의 인터페이스를 제공하는 웹 서버(web server)(5)와, 전자메일 전송을 지원하는 메일 서버(mail server)(6)와, 인터넷상에서 호스트명과 인터넷 프로토콜(IP) 주소 사이의 맵핑(mapping)과 변환을 지원하는 도메인 네임 시스템(DNS) 서버(7) 등과 같은 각종 서버들의 네트워크 연결을 제공한다. 또한 하나의 허브(3)는 도 1에 예시된 바와 같이 한 기업체의 전산실의 허브(8)와 그 기업체의 사무실의 허브(12)간의 네트워크 연결을 제공하고, 전산실내에 장착된 허브(8)는 업무용 각종 서버들(9~11)의 네트워크 연결을, 사무실내에 장착된 허브(12)는 바이러스 보호 컴퓨터(13)나 개인용 컴퓨터(14)나 보안 컴퓨터(15) 등의 네트워크 연결을 제공한다.

상기 종래의 네트워크 보호 시스템은 앞에서 설명된 시스템 보호를 위한 기술적 장치적 도구의 필수 구현 요소들을 실현하는데 사용되는 여러 기술들이 필수적으로 적용되며, 이외에 방화벽(2)을 사용하고 있다.

방화벽(2)은 내부 네트워크를 인터넷 등의 외부 네트워크로 연결하거나, 내부 네트워크(예로써, 특정 사업체의 랜)를 구축할 때 비인가된 외부 네트워크의 접근으로부터 내부 중요한 기밀이나 정보를 보호하기 위해 장착된다. 또한 방화벽(2)은 외부 네트워크와의 정보 송수신을 선택적으로 조정 허용하기 위한 하드웨어 또는 소프트웨어이다.

내부 네트워크와 외부 네트워크의 모든 통신은 방화벽(2)을 거쳐야 하며, 이 때 방화벽(2)은 네트워크간에 오가는 모든 통신을 감시하여 허용되지 않은 비인가 접근을 차단한다. 이를 통해 방화벽(2)은 불법적인 침입이나 해킹(특히 크래킹)으로부터 내부 네트워크를 보호한다. 다시 말해서 방화벽(2)은 인터넷과 특정 사업체 내의 랜(LAN : Local Area Network) 사이에 위치하여 보안을 담당한다.

그러나 최근에는 불법적인 침입의 형태가 다양해지고 있으며, 해킹(특히 크래킹)의 침입 패턴 또한 복잡하고 다양하게 변형되고 있기 때문에, 방화벽(2)을 네트워크 보호 수단으로써 운영한다 할지라도 침입의 위험이 따른다. 또한 방화벽(2)은 해킹(특히 크래킹)과 같은 불법적인 외부로부터의 침입을 막는 역할을 할뿐이고 내부 해킹을 차단할 수 없으며 또한 외부 해킹의 경우 그 근원지를 추적할 수 없기 때문에 보다 근본적인 보안을 위해서는 방화벽(2)과 함께 네트워크 보호 역할을 하는 강력한 또다른 보안 장비가 요구된다.

정리하면, 이상에서 설명된 종래의 기술에서 시스템 보호를 위해 사용되는 방화벽만으로는 키보드 유출과 같은 내부 사용자의 불법적인 행위나 외부로부터 들어오는 복잡하고 다양한 침입 패턴의 해킹(특히 크래킹)과 같은 불법적인 침입 행위를 막는다는게 역부족이다. 따라서 네트워크를 이용한 업무의 증가와 인터넷의 대중화로 국가나 기업, 그리고 개인의 해킹 사건 등 정보통신망을 통한 침해 사고가 계속 증가하고 있는 현 추세에서 네트워크 연결을 갖는 내부/외부 시스템으로부터 입출되는 정보를 감시하고 네트워크 연결을 갖는 대상 시스템에 대한 비인가/비정상적인 행위를 차단하는 보다 강력한 대처 방안이 필요하다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 상기한 점들을 감안하여 안출한 것으로, 네트워크 연결을 갖는 내부/외부 시스템으로부터 들어오고 나가는 정보를 실시간으로 감시하고, 네트워크 연결을 갖는 대상 시스템에 대한 비인가/비정상적인 행위를 자동 탐지 및 구별하여 차단함은 물론 그 근원지를 추적하는데 적당한 네트워크 보호 시스템을 제공하는데 있다.

본 발명의 또다른 목적은 본 발명의 실현을 위해, 네트워크 부하량에 영향을 미치지 않으면서 네트워크 보호 소프트웨어와 하드웨어가 일체형으로 그 설치와 사용이 용이한 네트워크 보호 시스템을 제공하는데 있다.

상기한 목적을 달성하기 위한 본 발명에 따른 네트워크 보호 시스템의 특징은, 각각 독립된 내부 네트워크와 외부 네트워크를 최적의 경로로 상호 연결시키는 라우터와, 상기 라우터에 의해 상호 연결된 경로를 통한 통신에 대해 일차적으로 감시하고 통제하는 방화벽과, 상기 방화벽에서 허가한 통신에 대해 실시간으로 감시하면서 비인가/비정상적인 통신을 구별 탐지하고, 그 탐지 내역으로부터 해당 네트워크 세션을 선택적으로 차단하고, 그 탐지 내역을 시각적 청각적으로 보고하고, 그 탐지 내역에 대한 정보를 관리하는 네트워크 보호 서버를 포함하여 구성된다.

바람직하게는, 웹 인터페이스를 통해 상기 네트워크 보호 서버에서 제공되는 네트워크 보호 어플리케이션을 원격지의 관리자가 실행시키기 위한 클라이언트 컴퓨터가 시스템에 더 구비된다.

특히 상기 네트워크 보호 서버는, 상기 내부 네트워크 내에서의 통신과, 상기 내부 네트워크와 상기 외부 네트워크간의 통신을 실시간으로 감시하기 위한 네트워크 감시 수단과, 상기 네트워크 감시 수단을 통해 감시되는 통신 중에서 상기 비인가/비정상적인 통신을 구별하고 탐지하기 위한 네트워크 탐지 수단과, 상기 네트워크 탐지 수단에 의해 탐지된 비인가/비정상적 통신을 차단하기 위한 접근 차단 수단과, 상기 네트워크 탐지 수단에 의한 비인가/비정상적 통신의 탐지 사실을 원격지의 관리자에게 유선 또는 무선으로 알리기 위한 경보 수단과, 상기 네트워크 탐지 수단에 의해 탐지된 그 탐지 내역의 보고서를 상기 원격지의 관리자에게 제공하기 위한 감시내역 보고 수단으로 구성된다.

상기 목적을 달성하기 위한 본 발명에 따른 네트워크 보호 시스템의 또다른 특징은, 특정 내부 네트워크 내에서의 통신과, 상기 내부 네트워크와 상기 외부 네트워크간의 통신을 실시간으로 감시하기 위한 네트워크 감시 엔진과, 상기 네트워크 감시 엔진을 통해 감시되는 통신 중에서 특정 해킹 패턴을 구별하고 탐지하기 위한 네트워크 탐지 엔진과, 상기 네트워크 탐지 엔진에 의해 탐지된 해킹을 차단하기 위한 접근 차단 엔진과, 상기 네트워크 탐지 엔진에 의한 해킹 탐지 사실을 원격지의 관리자에게 유선 또는 무선으로 알리기 위한 경보 엔진과, 상기 네트워크 탐지 엔진에 의해 탐지된 그 탐지 내역의 보고서를 상기 원격지의 관리자에게 제공하기 위한 감시내역 보고 엔진을 포함하는 네트워크 보호 서버와, 상기 네트워크 보호 서버의 상기 각 엔진들의 실행을 위한 웹 사이트를 웹 인터페이스 시켜주는 웹 서버로 구성되며, 상기 네트워크 보호 서버 및 상기 웹 서버의 구동 및 운영을 위한 운영체제로써 리눅스(LINUX)가 장착되어 사용된다.

바람직하게는, 상기 웹 인터페이스에 의한 상기 웹 사이트로의 접속을 지원하는 웹 브라우저를 내장하며, 상기 네트워크 보호 서버의 각 엔진들에 의한 어플리케이션을 실행하기 위한 사용자 인터페이스를 제공하는 상기 원격지 관리자의 컴퓨터가 더 구비된다.

발명의 구성 및 작용

이하, 본 발명에 따른 네트워크 보호 시스템에 대한 바람직한 일 실시 예를 첨부된 도면을 참조하여 설명

한다.

본 발명의 네트워크 보호 시스템은, 네트워크 연결을 갖는 내부/외부 시스템에서의 통신, 즉 내부 네트워크 자체에서 오가는 정보나 외부 네트워크와 오가는 정보를 24시간 실시간으로 감시하기 위한 감시 수단(monitoring)과, 실시간 감시를 통해 기밀 유출과 같은 내부 사용자의 불법적인 행위나 외부로부터 들어오는 복잡하고 다양한 침입 패턴의 해킹(특히 크래킹)과 같은 불법적인 침입 행위를 자동으로 탐지하고 구별하기 위한 탐지 수단(detecting)과, 탐지된 비인가/비정상적인 행위를 차단하기 위한 차단 수단(blocking)과, 비인가/비정상적인 행위가 탐지될 때 그 사실을 알리기 위한 경보 수단과(alarm), 일정 기간동안의 감시 및 탐지 내역과 로깅(logging)을 보고하기 위한 보고 수단(reporting)의 소프트웨어를 내장한 네트워크 보호 서버(이하에서는 '스나이퍼 리 칭함)를 구비한다. 여기서 스나이퍼(sniper)는 탐지된 불법 행위에 대한 주요 정보를 이메일(e-mail)이나 무선통신망을 등한 문자메시지서비스/음성메시지서비스를 통해 클라이언트(client)에게 알려주기 위한 수단을 구비한다.

또한 본 발명의 네트워크 보호 시스템은 외부로부터 들어오는 복잡하고 다양한 침입 패턴의 해킹(특히 크래킹)과 같은 불법적인 침입 행위를 자동으로 탐지하고 차단함은 물론 그 근원지를 추적하여 정확한 해킹 증거를 제공한다. 그리고 내부 네트워크에서의 기밀 유출과 같은 불법 행위나 비인가된 유해정보(음란 사이트, 카지노 사이트, 증권 사이트 등)의 웹 인터페이스를 감시 차단한다. 추가로 본 발명의 시스템은 키워드(keyword) 검색, 차단, 로깅을 통해 이메일 등을 통한 내부 정보 유출을 감시한다.

그리고, 본 발명의 네트워크 보호 시스템은 네트워크 부하량에 영향을 미치지 않는 패시브(passive) 방식을 채택하며, 네트워크 보호 소프트웨어와 하드웨어가 일체형으로 구현된다.

도 2는 본 발명에 따른 네트워크 보호 시스템의 전체 구성을 나타낸 도면으로, 전체적인 시스템 구성은 도 1과 유사하다. 따라서 본 발명의 스나이퍼(24,32)를 제외한 나머지 각 구성 요소들은 종래 기술에서 설명된 각 구성 요소들의 기능을 기본적으로 수행한다.

도 2를 참조하면, 먼저 본 발명의 시스템에 구비된 라우터(20)는 전송 패킷에 포함된 네트워크 주소를 근거로 하여 정보를 전송하며, 전송제어프로토콜/인터넷프로토콜(TCP/IP : Transmission Control Protocol/Internet Protocol) 등의 복수의 프로토콜을 지원한다. 또한 라우터(20)는 독립된 네트워크를 최적의 경로로 상호 연결한다.

본 발명의 네트워크 보호 시스템은 종래의 시스템과 마찬가지로 앞에서 설명된 시스템 보호를 위한 기술적 장치적 도구의 필수 구현 요소들을 실현하는데 사용되는 여러 기술들이 필수적으로 적용되며, 이외에 방화벽(21)과 스나이퍼(24,32)를 추가로 사용한다.

먼저 방화벽(21)은 외부 네트워크와의 정보 송수신을 선택적으로 조정 허용하기 위한 하드웨어 또는 소프트웨어로써, 내부 네트워크와 외부 네트워크의 모든 통신은 방화벽(2)을 거쳐야 한다. 그에 따라 방화벽(21)은 내부 네트워크를 인터넷 등의 외부 네트워크로 연결하며, 특정 사업체의 랜(LAN)과 같은 내부 네트워크를 구축할 때 장착되어 네트워크간에 오가는 모든 통신을 감시하고 허용되지 않은 비인가 접근을 차단함으로써 내부 중요한 기밀이나 정보를 1차적으로 보호한다.

다음 2차적인 네트워크 보호 서버인 스나이퍼(24,32)는 전산실의 허브(28)와 사무실의 허브(33)의 네트워크를 연결하는 허브(22)에 연결되며, 또한 특정 사이트를 제공하기 위한 웹 서버(web server)(25)나 전자메일 전송을 지원하는 메일 서버(mail server)(26)나 인터넷상에서 호스트명과 인터넷 프로토콜(IP) 주소 사이의 맵핑(mapping)과 변환을 지원하는 도메인 네임 시스템(DNS) 서버(27) 등과 같은 자유 링크를 갖도록 구성된 인터넷 비무장지대(Internet DMZ)에서의 각종 서버들(25,26,27)과 연결된다. 그 스나이퍼(24,32)는 도 4에 도시된 프로토콜 스택 구조로 정의된다.

스나이퍼(24,32)는 유닉스(UNIX) 클론(clone) 운영체계라고 할 수 있는 리눅스(LINUX)를 운영 시스템으로 사용한다.

스나이퍼(24,32)는 그 리눅스(LINUX)에 의해 동작하여 웹 환경의 인터페이스를 제공하는 웹 서버(미도시)를 포함하며, 컴퓨터를 통해 네트워크 보호를 위한 시스템을 원격 중앙 관리하는 시스템 관리자인 클라이언트(client)에게 네트워크 보호 사이트를 웹 인터페이스 시켜준다.

또한 스나이퍼(24,32)는 웹 인터페이스에 의한 네트워크 보호 사이트를 통해 여러 어플리케이션(application)을 수행한다. 그에 따른 어플리케이션 엔진으로는, 내부 네트워크에서의 통신 또는 외부 네트워크와의 통신, 다시 말해서 내부 네트워크 자체에서 오가는 정보나 외부 네트워크와 오가는 정보를 24시간 실시간으로 감시하기 위한 감시 엔진과, 실시간 감시를 통해 기밀 유출과 같은 내부 사용자의 불법적인 행위나 외부로부터 들어오는 복잡하고 다양한 침입 패턴의 해킹(특히 크래킹)과 같은 불법적인 침입 행위를 자동으로 탐지하고 구별하기 위한 탐지 엔진과, 탐지된 비인가/비정상적인 행위를 차단하기 위한 차단 엔진과, 비인가/비정상적인 행위가 탐지될 때 그 사실을 알리기 위한 경보 엔진과, 일정 기간동안의 감시 및 탐지 내역과 로깅(logging)을 보고하기 위한 보고 엔진이 있다. 또한 탐지된 불법 행위에 대한 주요 정보를 이메일(e-mail)이나 무선통신망을 통한 문자메시지서비스/음성메시지서비스를 통해 클라이언트(client)에게 알려주기 위한 어플리케이션 엔진이 더 존재한다.

다음 본 발명의 네트워크 보호 시스템은 내부 네트워크에서 여러 전송라인을 모아서 방화벽(21)을 통해 라우터(20)와 접속되는 하나의 허브(22)와, 특정 기업체 전산실의 각종 업무용 서버들(29,30,31)의 네트워크 연결을 제공하는 허브(29)와, 허브들(28,33)간의 연결을 제공하는 허브(22)에 의해 전산실의 허브(28)와 연결되며 바이러스 보호 컴퓨터(34)와 개인용 컴퓨터(35)와 보안 컴퓨터(36) 등의 네트워크 연결을 제공하는 또하나의 허브(33)와, 자유 링크를 갖도록 구성된 인터넷 비무장지대(Internet DMZ)에서의 웹 서버(web server)(25)와 메일 서버(mail server)(26)와 도메인 네임 시스템(DNS) 서버(27)와 같은 각종 서버들(25~27)의 네트워크 연결을 제공하는 또다른 허브(23)를 구비한다.

도 3은 본 발명의 일 실시 예에 따른 네트워크 보호 시스템의 구성을 나타낸 도면으로써, 특정 기업체의 적용 예를 나타낸 것이다.

도 3을 참조하면, 전체 네트워크 보호 시스템은 인터넷을 통해 관계회사의 컴퓨터(100)나 고객의 컴퓨터(110)나 해커의 컴퓨터(120)와의 상호 경로를 연결해주는 메인 라우터(130)와, 그 기업체에게 정한 보안 수준에 따라 메인 라우터(130)를 통과한 모든 통신을 1차적으로 감시하고, 그 기업체에게 정한 보안 수준에 어긋나는 특정 외부 네트워크 연결을 차단하는 방화벽(140)과, 도시된 특정 기업체의 내부 네트워크 시스템으로 구성된다. 도 3에서는 특정 기업체의 내부 네트워크 시스템이 본사, 별관 및 지점으로 분리된 내부 네트워크의 경우를 나타낸 것으로, 각 내부 네트워크(200,300,400)에는 본 발명의 네트워크 보호 서버인 스나이퍼(230,330,430)가 구비된다. 특히 본사 내부 네트워크(200)에는 자체 내부 네트워크 보호는 물론 별관 내부 네트워크(300)의 보호와 지점 내부 네트워크(400)의 보호를 위해 원격 중앙 관리하는 클라이언트 컴퓨터(240)가 구비된다.

본사 내부 네트워크(200)에는 방화벽(140)을 통과한 정보 대지 접속을 연결하는 집선 장치인 제1허브(210)가 구비된다. 그 제1허브(210)는 본사 내부 네트워크(200)의 내부 연결 및 다른 제1라우터(220)를 통해 연결되는 별관 내부 네트워크(300)의 연결과 지점 내부 네트워크(400)의 연결을 모아서 집속하는 또 다른 제2허브(211)와 연결되며, 또한 그 제1허브(210)에는 본 발명의 네트워크 보호 서버인 스나이퍼(230)와 원격 중앙 관리를 위한 클라이언트 컴퓨터(240)가 연결된다.

상기 제2허브(211)는 본사 내부의 여러 직원용의 개인용 컴퓨터들(260)의 연결을 집선하는 하나의 허브와 연결되며 또한 개인용 컴퓨터들(260)에게 웹 환경의 여러 인터페이스를 제공하는 웹 서버나 메일 서버와 같은 각종 업무용 서버와 데이터베이스와 연결된다.

별관 내부 네트워크(300)에는 별관 내부의 여러 직원용의 개인용 컴퓨터들(360)의 연결을 집선하는 제3허브(320)가 구비된다. 또한 그 제3허브(320)에는 개인용 컴퓨터들(360)에게 각종 업무에 관련된 웹 환경의 인터페이스를 제공하는 각종 업무용 서버(340,350)가 연결되며, 본사 내부 네트워크(200)의 제1라우터(220)와 상호 경로가 설정된 제2라우터(310)에 또한 연결된다. 특히 그 제3허브(320)에는 본 발명의 네트워크 보호 서버인 스나이퍼(330)가 연결된다.

다음 지점 내부 네트워크(400)의 내부 구성은 별관 내부 네트워크(300) 구성과 동일하므로 설명을 생략한다.

상기와 같이 특정 기업체에 적용하여 사용할 수 있는 본 발명의 네트워크 보호 시스템의 핵심은 네트워크 보호 서버인 스나이퍼(230,330,430)와 그 스나이퍼(230,330,430)에 내장된 각종 어플리케이션 엔진들을 구동시켜 원격에서 그 기업체 전체 네트워크를 관리하는 클라이언트 컴퓨터(240)이다.

이들 스나이퍼(230,330,430)와 클라이언트 컴퓨터(240)에 대해서는 도 4 내지 도 11을 통해 보다 상세히 설명한다.

도 4는 본 발명에 따른 네트워크 보호 시스템의 프로토콜 구조를 나타낸 도면으로써, 네트워크 보호 서버인 스나이퍼와, 그 스나이퍼와 연결되어 원격에서 시스템 전체의 네트워크를 관리하는 클라이언트 컴퓨터를 정의하기 위한 각 프로토콜 스택 구조를 나타낸 것이다.

스나이퍼의 프로토콜 스택 구조는 4개의 응용 계층들로 이루어지며, 클라이언트 컴퓨터의 프로토콜 스택 구조는 기본적으로 2개의 응용 계층들로 이루어진다. 이들 스나이퍼와 클라이언트 컴퓨터간에는 물리계층(physical layer)으로써 랜(LAN) 접속과 인터넷 접속을 지원하는 전송제어프로토콜/인터넷프로토콜(TCP/IP)이 정의된다.

스나이퍼의 프로토콜 계층 중에서 제1계층(510)은 운영 시스템 계층(OS layer)으로써, 리눅스(LINUX)를 사용하도록 정의한다. 다음 제2계층(520)은 스나이퍼를 위한 웹 서버(Web server)를 정의한다. 다음 제3계층(530)은 여러 어플리케이션 엔진들을 정의하는데, 그 어플리케이션 엔진들은 네트워크 감시, 네트워크 탐지, 서버 접근 차단, 경보, 이메일, 보고 등의 기능을 수행토록 정의된다. 다음 제4계층(540)은 여러 어플리케이션들을 정의하는데, 그 어플리케이션들은 본 발명의 네트워크 보호 어플리케이션, 데이터베이스 연동 어플리케이션, 그리고 확장 가능한 어플리케이션을 정의한다.

다음 클라이언트 컴퓨터의 프로토콜 계층 중에서 제1계층(610)은 운영 시스템 계층(OS layer)으로써, 윈도우즈 95나 윈도우즈 98이나 윈도우즈 2000이나 윈도우즈 엔티(windows NT)를 사용하도록 정의한다. 다음 제2계층(620)은 사용자 인터페이스 계층으로써, 웹 브라우저(web browser : 예로써, 인터넷 익스플로러 5.0 버전(version)이나 넷스케이프 네비게이터)를 정의한다.

상기와 같이 정의되는 프로토콜 스택 구조를 근거로 하여 구현되는 본 발명의 핵심 구성에 대해 다음 도 5를 참조하여 설명한다.

도 5는 본 발명에 따른 네트워크 보호 시스템의 네트워크 보호 서버의 내부 구성과 클라이언트 컴퓨터를 나타낸 블록도이다.

클라이언트 컴퓨터(600)는 윈도우즈 95(windows 95)나 윈도우즈 98(windows 98)이나 윈도우즈 2000(windows 2000)이나 윈도우즈 엔티(windows NT) 중 하나의 운영체계를 사용한다. 이들 중 하나의 운영체계에 의해 동작하며 전송제어프로토콜/인터넷프로토콜(TCP/IP) 통신을 통해 본 발명의 네트워크 보호 사이트에 접속하기 위한 웹 브라우저(web browser)가 클라이언트 컴퓨터(600)에 내장된다.

네트워크 보호 서버인 스나이퍼(500)는 리눅스(LINUX) 운영체계를 사용하며, 상기 클라이언트 컴퓨터(600)로 본 발명의 네트워크 보호 사이트를 제공하기 위한 웹 서버가 기본적으로 구비된다. 특히 도 5에 도시된 네트워크 보호 서버(500)의 내부 블록들은 본 발명의 시스템에 의해 수행되는 네트워크 보호 어플리케이션에 관련된 것들이다.

네트워크 보호 어플리케이션을 실행하기 위한 네트워크 보호 서버(500)의 내부 구성은, 네트워크 감시부(531)와, 네트워크 탐지부(532)와, 접근 차단부(533)와, 경보 제공부(534)와, 감시 내역 보고부(535)를 포함하여 구성된다.

네트워크 감시부(531)는 내부 네트워크에서의 통신을 24시간 실시간으로 감시하거나 미리 정해진 옵션에

따라 그 정해진 시간대별로 감시하고, 외부 네트워크에서 내부 네트워크로의 통신이나 내부 네트워크에서 외부 네트워크로의 통신을 24시간 실시간 또는 정해진 시간대별로 감시한다. 이 때 외부 네트워크와 내부 네트워크간의 통신의 하나의 예로써 전송제어프로토콜/인터넷프로토콜(TCP/IP) 통신의 경우에는 전송제어 프로토콜(TCP) 세그먼트(segment)의 헤더(header)를 분석하고 또한 인터넷프로토콜(IP) 데이터그램(datagram)의 헤더(header)를 분석하여 감시한다. 또한 네트워크 감시부(531)는 원격지로부터 접근하는 사용자 명령어를 실시간으로 감지한다.

네트워크 탐지부(532)는 네트워크 감시부(531)와 연계되어 동작하며, 네트워크 감시부(531)의 실시간 감시를 통해 내부 네트워크에서 외부 네트워크로의 기밀 유출과 같은 내부 네트워크 불법 행위나 외부 네트워크에서 내부 네트워크로의 해킹(특히 크래킹)과 같은 불법적인 침입 행위를 자동으로 탐지하고 구별한다.

하나의 예로써 네트워크 감시부(531)와 네트워크 탐지부(532)는 네트워크 데이터를 스캔(scan)하고 캡쳐(capture)하는 수동방식에 의해 감시하고, 그 감시를 통해 내부 네트워크 불법 행위나 외부의 해킹에 의한 접근이라고 판단되면, 다음에 설명될 접근 차단부(533)를 통해 그 네트워크 세션(network session)을 차단한다.

다음 접근 차단부(533)는 네트워크 탐지부(532)에서 내부 네트워크 불법 행위나 외부 해킹이 탐지될 경우, 그 해당 네트워크 세션을 차단한다.

다음 경보 제공부(534)는 내부 네트워크 불법 행위나 외부 해킹이 탐지될 경우, 그 사실을 클라이언트에게 경보한다. 이 때는 클라이언트 컴퓨터(600)의 화면에 시각적으로 청각적으로 알려주는 방법과, 이메일(e-mail)이나 무선통신망을 통한 문자메시지서비스/음성메시지서비스를 통해 클라이언트(client)에게 알려주는 방법이 있다. 본 발명의 네트워크 보호 서버(500)에는 이러한 각 경보 방법을 실현시키기 위한 장비를 구비한다.

다음 감시 내역 보고부(535)는 네트워크 감시부(531)와 네트워크 탐지부(532)에 의한 일정 기간동안의 감시 및 탐지 내역과, 로깅(logging)을 보고한다.

그밖에도 본 발명의 네트워크 보호 서버(500)는 네트워크 탐지부(532)에 의해 내부 네트워크 불법 행위나 외부 해킹이 탐지될 경우에 해커의 침입 경로를 라우터 단위로 추적하는 추적 수단을 더 구비하며(여기서, 본 발명의 네트워크 보호 서버는 해커의 침입 경로를 추적하고 그 경로를 해당 지도에 맵핑시켜 클라이언트에게 시각적으로 보여준다.), 또한 하드디스크(HDD)에 구축된 데이터베이스와 연동하여 감사 및 탐지 내역에 대한 주요 정보를 관리하고, 상기 감시 내역 보고부(535)의 보고 내용을 종합적으로 관리하는 관리 수단을 더 구비한다.

다음은 네트워크 보호 서버(500)의 내부 구성 요소들의 보다 상세한 동작을 이하 도 6 내지 도 11을 참조하여 설명한다.

이하의 도 6 내지 도 11은 네트워크 보호 서버의 웹 서버가 클라이언트 컴퓨터에 네트워크 보호 사이트를 웹 인터페이스 저겨줌으로써 디스플레이되며, 각각 도시된 화면 포맷을 통해 클라이언트가 본 발명의 네트워크 보호 어플리케이션을 실행한다.

클라이언트 컴퓨터에 표시되는 네트워크 보호 어플리케이션의 메뉴 팔레트(manu palette)로는 실시간 모니터, 최근 모니터, 탐지/차단/경보, 주요정보관리, 종합보고서, 환경설정, 도움말 등이 있다.

도 6은 본 발명에서 외부 및 내부 접근 내역을 감시하기 위한 클라이언트 컴퓨터의 화면 포맷을 나타낸 도면으로, 원격 중앙 관리자만 클라이언트는 실시간 모니터 팔레트를 선택하고 그에 따라 디스플레이되는 도 6의 화면을 통해 현재 내부 네트워크의 사용 내역 및 외부 네트워크의 사용 내역을 실시간으로 감시한다. 즉, 클라이언트 컴퓨터에는 현재 내부 네트워크 또는 외부 네트워크를 사용하고 있는 전체 컴퓨터와 사용 포트(port)와 작업 형태 및 사용시간과 데이터 전송량 등의 종합적인 정보 테이블이 디스플레이되며, 그 종합적인 정보 테이블을 토대로 제작되는 차트가 디스플레이된다.

특히 디스플레이되는 종합 정보 테이블은 컴퓨터별, 사용자별, 서비스별로 상세 내역을 검색할 수 있는데, 그 상세한 항목은 외부사용자의 내부 네트워크 서버 사용 내역, 내부사용자의 외부 네트워크 서버 사용 내역, 내부사용자의 내부 네트워크 서버 사용 내역, 전체사용자의 시스템 전체 서버 사용 내역으로 분류된다. 따라서 클라이언트가 상세 항목(외부사용자-내부서버, 내부사용자-외부서버, 내부사용자-내부서버, 전체사용자-전체서버) 중에서 하나의 옵션을 선택함에 따라, 여러 사용자와, 그 여러 사용자에 의해 사용되고 있는 각 서버와, 그 여러 사용자가 각 서버로부터 주고받는 각 데이터 사용량과, 그 여러 사용자의 각 서버 사용시간 및 그 사용자들에 대한 각 정보가 하나의 테이블화되어 실시간으로 디스플레이된다.

이러한 도 6의 화면을 통해 클라이언트는 전체 네트워크를 자세히 감시한다. 특히 클라이언트가 종합 정보 테이블에서 상세 항목 중 하나(도 6에서는 예로써 내부사용자-외부서버)를 선택(click)하면, 클라이언트는 컴퓨터 원격 접속 서비스를 지원하는 텔넷(TELNET)을 통해 네트워크 보호 서버인 소나이퍼의 네트워크 감시부에서 감시하고 있는 현재 상세 자료를 온라인으로 검색하며, 그 검색 자료는 원격지 사용자 명령어이다.

도 7은 본 발명에서 내부 네트워크를 사용한 외부 사용자의 정보를 클라이언트 컴퓨터의 화면에 나타낸 도면으로써, 원격 중앙 관리자인 클라이언트는 최근 모니터 팔레트를 선택하고 그에 따라 디스플레이되는 도 7의 화면을 통해 내부 네트워크의 사용 내역 및 외부 네트워크의 사용 내역을 정해진 시간대별로 감시한다.

즉 클라이언트 컴퓨터에는 정해진 특정 시간동안 내부 네트워크 또는 외부 네트워크를 사용한 주요 정보(도메인, 인터넷프로토콜(IP) 주소, 사용량, 접속건 수, 사용시간, 접속시간, 사용자 정보 등)에 대한 정보 테이블이 도 7a와 같이 디스플레이되며, 그 정보 테이블을 토대로 제작된 도 7b의 차트가 디스플레이된다.

특히 디스플레이되는 정보 테이블은 컴퓨터별, 사용자별, 서비스별로 상세 내역을 검색할 수 있는데, 그 상세한 항목은 내부 서버의 사용 내역, 외부 서버의 사용 내역, 내부 사용자의 사용 내역 및 외부 사용자의 사용 내역으로 분류된다. 따라서 클라이언트가 상세 항목(내부서버, 외부서버, 내부사용자, 외부사용자) 중에서 하나의 옵션을 선택함에 따라, 도메인과 인터넷 프로토콜(IP) 주소와 사용량과 접속건 수와 사용시간과 접속시간과 사용자 정보에 대한 정해진 최근 시간등만의 자료가 테이블화되어 디스플레이된다.

이러한 도 7의 화면을 통해 클라이언트는 최근 전체 네트워크를 감시한다.

도 8은 본 발명에서 해킹 정보들과 그의 조치방법을 클라이언트 컴퓨터의 화면에 나타낸 도면으로, 원격 중앙 관리자인 클라이언트는 '탐지/차단/경보' 팔레트를 선택하고 내부 네트워크 및 외부 네트워크를 실시간 감시하여 탐지된 해킹 정보들과 그의 조치방법을 도 8의 화면을 통해 출력한다.

즉 클라이언트 컴퓨터에는 탐지된 해킹 정보로써, 해킹주체(공격자), 해킹대상(대상자), 현재 해킹의 진행상태(상태), 시도횟수, 조치(차단 또는 경보), 공격시간(시작과 종료), 공격자 정보들에 대한 정보 테이블이 도 8a와 같이 디스플레이되며, 도 8b와 같이 도 8a의 정보 테이블을 토대로 클라이언트에 의해 선택된 정보 목록에 대해서만 디스플레이된다.

특히 디스플레이되는 정보 테이블에서 클라이언트가 정보 테이블의 한 목록을 선택(click)할 경우에는 해킹주체의 공격 방법에 대한 해설과 그 조치방법이 실시간 표시된다. 즉 해당 해킹의 종류 및 해킹대상에 미치는 위험도는 물론 그의 대응 방법을 설명해준다.

도 8의 정보 테이블 또한 컴퓨터별, 사용자별, 서비스별로 상세 내역을 검색할 수 있는데, 그 상세한 항목은 외부사용자의 내부 네트워크 서버 사용 내역, 내부사용자의 외부 네트워크 서버 사용 내역, 내부사용자의 내부 네트워크 서버 사용 내역, 전체사용자의 시스템 전체 서버 사용 내역으로 분류된다. 따라서 클라이언트가 상세 항목(외부사용자-내부서버, 내부사용자-외부서버, 내부사용자-내부서버, 전체사용자-전체서버) 중에서 하나의 옵션을 선택함에 따라, 탐지된 해킹 정보가 테이블화되어 실시간으로 디스플레이된다.

이러한 도 8의 화면을 통해 클라이언트는 해킹 근원지 추적에 대한 공격자의 상세정보를 제공받는다. 특히 본 발명의 네트워크 보호 시스템은 해킹 근원지 추적을 위해 탐지되는 모든 외부사용자 및 외부서버의 정보를 의뢰하기 위한 미국의 인터닉(Internic), 아시아 인터넷 정보센터(apnic), 한국 인터넷 정보센터(knic) 등의 공식 센터와 연결되는데, 이들 공식 센터들은 인터넷의 도메인 네임 시스템(DNS) 정보를 관리한다. 본 발명의 네트워크 보호 시스템은 그 공식 센터에 해킹 근원지 정보를 의뢰하고, 그 공식 센터로부터 제공받은 해킹 근원지 정보를 토대로 캐쉬 테이블(cache table)을 구축한 다음 이를 클라이언트에게 보여준다.

도 9는 본 발명에서 유해정보 차단 설정과 실시간 내부 서버 접속 감시를 위한 클라이언트 컴퓨터의 화면 포맷을 나타낸 도면으로, 원격 중앙 관리자인 클라이언트는 '주요 정보 관리' 팔레트를 선택하고 그에 따라 디스플레이되는 도 9a의 화면을 통해 본 발명의 네트워크 보호를 위한 정보 차단 설정을 수행하며, 도 9b의 화면을 통해 실시간으로 내부 서버 접속을 감시한다.

물론 도 9a는 항목 중에서 '정보 차단 설정' 항목을 선택함에 따른 화면이며, 그밖에도 'E-MAIL과 상세내역' 항목이 있다. 따라서 본 발명에서는 도 9a를 통해 이메일에 대한 송수신 내역(이메일 발송자 및 접수자에 대한 정보 등)을 관리하며, 이메일의 내용(본문 및 첨부파일)을 검열하고 정해진 특정 문자열(특히 기밀정보) 발송을 차단할 수 있도록 클라이언트에 의해 설정된다.

또한 도 9b의 화면을 통해 실시간으로 내부 서버 접속을 감시하는데, 즉 그 내부 네트워크 세션(network session)을 감시한다.

특히 도 9의 화면을 통해 내부사용자의 텔넷(TELNET), 파일전송프로토콜(FTP ; File Transfer Protocol), Rologin 등의 사용에 대한 상세 내역을 관리하고, 허가되지 않은 웹 사이트(음란 사이트, 카지노 사이트, 증권 사이트 등)에 대한 접속을 관리하고 그를 차단한다. 또한 클라이언트는 도 9를 통해 내부 네트워크에서 여러 개인용 컴퓨터의 하드디스크를 공유할 때 그에 따른 통제 관리를 수행하며, 특정 서버의 접근 차단과 서비스 차단 설정을 통해 네트워크를 통제한다.

도 10은 본 발명에서 다양한 조건 검색 및 그의 결과에 따른 각종 보고서를 클라이언트 컴퓨터의 화면에 나타낸 도면으로, 원격 중앙 관리자인 클라이언트는 '종합보고서' 팔레트를 선택하고 내부 네트워크 및 외부 네트워크를 실시간 또는 정해진 시간대별로 감시한 내역이나, 해커 대응 방법이나, 자료 내역이나, 사용 내역을 테이블화하여 도 10a를 통해 보고하며, 그 테이블을 토대로 제작된 도 10b의 차트가 디스플레이된다.

특히 디스플레이된 도 10a의 테이블은 특정일시/사용자/서버의 다양한 조건(또한 컴퓨터별, 서비스별, 기간별, 개인 또는 그룹별, 월별, 일별, 시간대별에 대한 통계)으로 검색되며 해당 네트워크 서버 접근에 대한 정보 보고서 형태로 작성된 후 도 10a와 같은 화면뿐만 아니라 도 10b와 같은 차트 디스플레이 또는 프린터 출력에 의해 보고된다.

도 11은 본 발명에 따른 네트워크 보호 시스템의 마스터 관리와, 실시간 감시 네트워크 데이터 선별 로깅 관리를 위한 클라이언트 컴퓨터의 화면을 나타낸 도면으로, 본 발명의 스나이퍼에 의한 사용자 관리, 네트워크 내부 컴퓨터 관리, 로깅 설정 및 하드디스크 자료 설정 등의 환경설정을 위한 것이다.

즉, 클라이언트는 스나이퍼 사용자의 마스터 관리를 위해, 사용자 식별번호(ID)에 인터넷프로토콜(IP) 주소를 등록한 후 특정 사용자에서만 접속이 가능하도록 하는 기능을 지원한다.

또한 클라이언트는 네트워크 내부 컴퓨터 관리를 통해 인터넷프로토콜(IP) 주소를 임의로 수정하여 서버의 자료를 유출시키는 행위를 확인할 수 있으며, 로깅 설정을 통해 네트워크 데이터를 실시간으로 감시하여 선별하는 로깅(logging) 기능을 수행한다. 또한 클라이언트는 윈도우즈 95나 윈도우즈 98이나 윈도우즈 2000이나 윈도우즈 엔티(Windows NT)에서의 하드디스크 공유를 통제한다.

상기에서 도 6 내지 도 11을 통해 설명된 클라이언트 컴퓨터를 통해 수행되는 모든 동작은 스나이퍼가 웹 인터페이스를 통해 제공하며, 따라서 스나이퍼에는 클라이언트 컴퓨터 화면을 통해 수행되는 모든 동작을 수행하기 위한 소프트웨어가 내장되어 다음에 종합적으로 나열된 능력을 갖는다.

첫 째, 실시간 감시 및 최근 감시 능력이다. 이는 실시간 또는 정해진 시간대별로 내부/외부 네트워크 사용 내역을 감시하며, 특히 옵션으로 컴퓨터별, 사용자별, 서비스별로 구분하여 상세 내역을 검색할 수 있다. 그 감시 결과는 테이블로 클라이언트 컴퓨터에 디스플레이되는데, 외부사용자-내부장비, 내부사용자-내부서버, 내부사용자-외부서버, 전체사용자로 각각 구분되어 디스플레이되며, 디스플레이되는 자료는 서버, 사용자, 사용량, 사용시간, 네트워크 부하량, 사용자 정보 등이다. 이러한 실시간 감시 및 최근 감시 능력을 통해 실시간으로 원격지 사용자의 명령어를 감지하고 차단할 수 있다.

둘 째, 해킹탐지/차단/경보 능력이다. 이는 실시간으로 해킹을 탐지한 후 네트워크를 차단하고, 이메일(e-mail)이나 무선통신망을 이용한 문자메시지 서비스 또는 음성메시지 서비스를 사용하여 해킹 탐지 사실 및 그 해킹 정보를 실시간으로 원격 중앙 관리자의 클라이언트에게 알려주는 능력이다. 여기서 경보되는 해킹 정보로는 공격자, 대상자, 전행사항, 차단사항 등이며, 네트워크 보호 서버인 스나이퍼는 여러 패턴의 해킹 공격에 대한 해쉬 및 그의 대응 방안을 또한 알려준다. 특히 스나이퍼는 해킹 근원지를 실시간으로 추적할 수 있도록 상세한 공격자 정보를 제공한다.

세 째, 주요 정보 관리 능력이다. 이는 내부 네트워크 사용자의 이메일(e-mail)에 대한 송수신 내역(발송자, 접수자, 이메일 내용 등)을 검열하고 관리하며, 특히 이메일을 통한 특정 문자열(기밀정보)을 검열하여 이를 전송 차단한다. 또한 텔넷이나 파일전송프로토콜(FTP)이나 Rologin 등에 대한 상세 내역을 관리하고, 허가되지 않은 웹 사이트(음란 사이트와 같은 유해 사이트, 카지노 사이트, 증권 사이트 등)들의 유해 정보를 관리하고, 내부 네트워크 개인용 컴퓨터의 하드디스크 공유에 대해 통제하고 관리한다.

네 째, 종합보고서 관리 능력이다. 이는 실시간 또는 정해진 시간대별 감시 내역에 대한 보고서, 해커의 침입/차단/경보 및 그에 방지 대책 보고서, 이메일(e-mail)이나 텔넷(TELNET)이나 파일전송프로토콜(FTP)이나 Rologin 등의 자료 송수신 내역 보고서 등을 다양한 형태(화면을 통한 테이블이나 차트, 프린터 출력)로 제공한다. 여기서 보고서는 컴퓨터별, 서비스별, 기간별, 개인/그룹별 등에 따라 구분되며, 또한 그 구분 항목에서 월별, 일별, 시간대별 등계 자료를 제공한다.

다섯 째, 환경 설정 능력이다. 이는 사용자 마스터 관리와 네트워크 내부 컴퓨터를 관리하기 위한 설정과, 로깅 설정을 수행하는 능력이다.

그밖에도 본 발명의 네트워크 보호 시스템에서 네트워크 보호 서버인 스나이퍼는 내부 네트워크 사용자의 인터넷 접속을 통제하는데, 이를 위해 스나이퍼는 내부 사용자에 대한 랜카드(lancard)의 유일 하드웨어 주소(MAC 주소)와 인터넷프로토콜(IP) 주소를 자동 또는 수동으로 구축한 다음 클라이언트가 내부 사용자에 대한 인터넷 사용 허가 또는 금지를 설정함에 따라서 그 접속을 통제한다.

다음 본 발명의 네트워크 보호 시스템에서 네트워크 보호 서버인 스나이퍼는 내부/외부 사용자가 서버에 접근한 내역을 관리하는데, 즉 내부/외부 사용자가 서버에 접근하여 사용한 내역을 모두 로깅할으로써 언제, 어떤 작업을 했는지에 대한 내역을 관리한다. 이에 따라 기밀정보의 유출 경로 및 해킹으로 인한 피해를 신속하게 복구할 수 있도록 해주며, 또한 그 내역을 해킹 추적 정보로써 사용한다.

다음은 여러 침입 패턴의 해킹 공격과, 그 해킹 공격에 대해 상기 나열된 능력을 갖는 네트워크 보호 서버인 스나이퍼의 내장 프로그램을 사용한 대처 방법에 대해 설명한다. 다음 설명을 위해 도 12에 도시된 인터넷프로토콜(IP) 데이터그램의 구조와, 도 13에 도시된 전송제어프로토콜(TCP) 세그먼트의 구조를 참조한다.

도 12에서 인터넷프로토콜(IP) 데이터그램은, 인터넷프로토콜(IP) 버전을 나타내기 위한 4비트와, 인터넷프로토콜(IP) 헤더 길이를 나타내기 위한 4비트와, 송신하고 있는 인터넷프로토콜(IP)의 서비스 타입(TOS : Type Of Service)를 나타내기 위한 8비트와, 인터넷프로토콜(IP) 데이터그램의 전체 길이(헤더+데이터)를 나타내기 위한 16비트와, 인터넷프로토콜(IP) 데이터그램의 소속 표시를 나타내는 식별자(Identification)의 16비트와, 분할(fragmentation) 여부 표시를 나타내는 플래그(flag)의 4비트와, 분할된 데이터그램의 위치 표시를 나타내는 분할 옵셋(fragmentation offset)의 12비트와, 인터넷프로토콜(IP) 데이터그램이 네트워크에 머물 수 있는 시간 지정(Time of live)을 위한 8비트와, 상위계층(higher layer) 프로토콜의 종류에 대한 정보를 나타내기 위한 프로토콜의 8비트와, 인터넷프로토콜(IP) 데이터그램 헤더에 대한 에러 검사를 위한 헤더 체크섬(header checksum)의 16비트와, 송신측 인터넷프로토콜(IP) 주소를 나타내기 위한 출발지 주소(source address)의 32비트와, 수신측 인터넷프로트콜(IP) 주소를 나타내기 위한 목적지 주소(destination address)의 32비트를 포함한 20바이트(byte)의 헤더와, 수십 바이트의 데이터로 구성된다.

다음 도 13에서 전송제어프로토콜(TCP) 세그먼트는, 출발지 포트 번호(source port number)의 16비트와, 목적지 포트 번호(destination port number)의 16비트와, 송신하는 데이터스트림(data stream)의 바이트 번호를 나타내는 시퀀스 번호(sequence number)의 32비트와, 다음에 수신할 것을 기대하는 데이터스트림의 번호를 나타내는 승인 번호(acknowledgement number)의 32비트와, 전송제어프로토콜(TCP) 세그먼트의 헤더 길이를 나타내는 4비트와, 모두 '0'의 비트값을 갖는 예약(reserved)의 6비트와, 전송제어프로토콜(TCP) 세그먼트의 종류들을 표시하는 제어 플래그(control flag)의 6비트와, 수신측의 현재 가용 버퍼 크기를 나타내기 위한 윈도우 크기(window size)의 16비트와, 전송제어프로토콜(TCP) 세그먼트의 무결성(integrity) 검사를 위한 체크섬(checksum)의 16비트와, 긴급 데이터의 범위를 표시하기 위한 어젠트 포인터(urgent pointer)의 16비트를 포함하는 20바이트(byte)의 헤더와, 옵션(option)과 데이터(data)로 구성된다.

특히 전송제어프로토콜(TCP) 세그먼트의 제어 플래그는, 어젠트 포인터(urgent pointer) 필드가 유효함을 표시하는 'URG'와, 승인 번호(acknowledgement number) 필드가 유효함을 표시하는 'ACK'와, 전송제어프로토콜(TCP) 세그먼트를 만들지 않고 처리하는 푸쉬(push) 요구를 위한 'PUSH'와, 비정상적인 연결의 종료 요구를 위한 'RST(reset)'와, 초기 연결 설정 요구를 위한 'SYN'과, 연결 해제 요구를 위한 'FIN'으로 구

분된다.

-제1패턴-

공격명 : 에스와이엔 플러딩(SYS Flooding)

공격방법 : 도스(DOS) 공격의 한 방법으로서 인터넷프로토콜(IP) 주소를 바꿔서 이를 통해 해킹하는 인터넷프로토콜 스푸핑(IP Spoofing) 공격을 하기 위한 방법으로 사용되기도 한다. 이는 전송제어프로토콜(TCP) 세그먼트를 이용하여 공격자가 대상 서버에 접속을 시도할 때 전송제어프로토콜(TCP) 세그먼트의 헤더에 초기 연결 설정 요구를 위한 제어 플래그인 'SYN'을 온(on)하여 보내면, 대상 서버는 이에 대한 답변으로 'SYN/ACK'을 보낸다. 이후 공격자는 승인(ACK)을 받는다는 점을 이용하여, 임의로 자신의 인터넷 프로토콜(IP) 주소를 속여 응답을 할 수 없는 다량의 인터넷프로토콜(IP) 주소를 대상 서버에 보내면, 그 대상 서버는 공격자에게 그에 따라 각각 'SYN/ACK'을 모두 보내고 그에 대한 승인(ACK)을 받기 위해 대상 서버측의 대기 상태에 있게 된다. 공격자는 이 대기 상태를 이용하여 공격한다.

탐지방법 : 본 발명에서는 공격자가 보내는 'SYN' 신호와 그 신호에 대한 대상 서버의 승인('SYN/ACK')을 계산한다. 그 때 'SYN'이 과도하게 발생한다는 점을 이용하여 탐지한다.

조치방법 : 1. 공격자가 대상 서버에 요구한 'SYN'의 개수만큼 본 발명의 네트워크 보호 서버(SNIPER)가 대상 서버에게 연결을 초기화시키는 리셋(RESET) 신호를 보내어 대기 상태에서 벗어나고 그 대상 서버를 정상화시킨다.

2. 원격 중앙 관리자인 클라이언트는 대상 서버의 연결 큐 크기(Connect Queue Size)를 증가시키거나, 대상 서버 사용시간에 제한을 두거나(Time Out 줄임), 운영체계(OS)의 버전을 높여서 공격의 피해를 최소화한다.

-제2패턴-

공격명 : 에스와이엔 포트 스캔(SYN Port Scan)

공격방법 : 해킹을 위해 대상 서버(또는 대상 컴퓨터)가 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 어떤 포트를 오픈(Open)하여 서비스하고 있는지를 알아내어 공격하는 방법으로, 그 포트 번호 0번부터 65,535번까지의 포트에 순차적 또는 무순위로 초기 연결 설정 요구를 위한 제어 플래그인 'SYN' 신호를 보내어 대상 서버가 응답하는 승인(SYN/ACK)을 확인한다.

탐지방법 : 특정 공격자(해커)가 특정 대상 서버에게 포트를 달리하여 보내는 'SYN'의 개수를 계산하여, 일정량 이상의 'SYN'을 보내는 것으로 판단되면 포트 스캔(Port Scan)으로 분류한다.

조치방법 : 본 발명의 네트워크 보호 서버(SNIPER)는 원격 중앙 관리자인 클라이언트에게 포트 스캔 발생 사실을 알리고, 그에 따라 클라이언트는 대상 서버의 불필요한 서비스 포트를
디스에이블(Disable)시킨다. 그로써 해킹 공격을 최소화한다.

-제3패턴-

공격명 : 널 포트 스캔(NULL Port Scan)

공격방법 : 해킹을 위해 대상 서버(또는 대상 컴퓨터)가 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 어떤 포트를 오픈(Open)하여 서비스하고 있는지를 알아내어 공격하는 방법으로, 그 포트 번호 0번부터 65,535번까지의 포트에 순차적 또는 무순위로 의미없는 널(NULL) 신호를 보내어 대상 서버가 응답하는 리셋(RESET) 신호를 확인한다.

탐지방법 : 특정 공격자(해커)가 특정 대상 서버에게 포트를 달리하여 보내는 널(NULL)의 개수를 계산하여, 일정량 이상의 널(NULL)을 보내는 것으로 판단되면 포트 스캔(Port Scan)으로 분류한다.

조치방법 : 본 발명의 네트워크 보호 서버(SNIPER)는 원격 중앙 관리자인 클라이언트에게 포트 스캔 발생 사실을 알리고, 그에 따라 클라이언트는 대상 서버의 불필요한 서비스 포트를
디스에이블(Disable)시킨다. 그로써 해킹 공격을 최소화한다.

-제4패턴-

공격명 : 핀 포트 스캔(FIN Port Scan)

공격방법 : 해킹을 위해 대상 서버(또는 대상 컴퓨터)가 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 어떤 포트를 오픈(Open)하여 서비스하고 있는지를 알아내어 공격하는 방법으로, 그 포트 번호 0번부터 65,535번까지의 포트에 순차적 또는 무순위로 연결 해제 요구를 위한 제어 플래그인 'FIN' 신호를 보내어 대상 서버가 응답하는 리셋(RESET) 신호를 확인한다.

탐지방법 : 특정 공격자(해커)가 특정 대상 서버에게 포트를 달리하여 보내는 'FIN'의 개수를 계산하여, 일정량 이상의 'FIN'을 보내는 것으로 판단되면 포트 스캔(Port Scan)으로 분류한다.

조치방법 : 본 발명의 네트워크 보호 서버(SNIPER)는 원격 중앙 관리자인 클라이언트에게 포트 스캔 발생 사실을 알리고, 그에 따라 클라이언트는 대상 서버의 불필요한 서비스 포트를
디스에이블(Disable)시킨다. 그로써 해킹 공격을 최소화한다.

-제5패턴-

공격명 : 엑스마스 포트 스캔(XMAS Port Scan)

공격방법 : 해킹을 위해 대상 서버(또는 대상 컴퓨터)가 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 어떤 포트를 오픈(Open)하여 서비스하고 있는지를 알아내어 공격하는 방법으로, 그 포트 번호 0번부터 65,535번까지의 포트에 순차적 또는 무순위로 연결 해제 요구를 위한 제어 플래그인 'FIN' 신호나, 긴급 데이터 표시(urgent pointer) 필드가 유효함을 나타내는 제어 플래그인 'URG' 신호나, 푸쉬(push) 요구를 위한 제어 플래그인 'PUSH' 신호를 보내어 대상 서버가 응답하는 리셋(RESET) 신호를 확인한다.

탐지방법 : 특정 공격자(해커)가 특정 대상 서버에게 포트를 달리하여 보내는 'FIN'의 개수나 'URG'의 개수나 'PUSH'의 개수를 계산하여, 일정량 이상의 'FIN', 'URG', 'PUSH'를 보내는 것으로 판단되면 포트 스캔(Port Scan)으로 분류한다.

조치방법 : 본 발명의 네트워크 보호 서버(SN(PBR)는 원격 중앙 관리자인 클라이언트에게 포트 스캔 발생 사실을 알리고, 그에 따라 클라이언트는 대상 서버의 불필요한 서비스 포트를 디스에이블(Disable)시킨다. 그로써 해킹 공격을 최소화한다.

-제6패턴-

공격명 : 핑거프린트(FingerPrint : OS Scan)

공격방법 : 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 패킷을 구현함에 있어서 운영체계(OS)마다 구현 방식이 다르다는 점을 이용하여 여러 가지 전송제어프로토콜/인터넷프로토콜(TCP/IP) 패킷을 특정 대상 서버에 보내어 응답되는 패킷을 분석함으로써, 그 대상 서버의 운영체계(OS)를 파악한 다음 해킹의 자료로 사용한다.

탐지방법 : 특정 사용자가 대상 서버에 보내는 전송제어프로토콜/인터넷프로토콜(TCP/IP) 패킷 중에서 전송제어프로토콜(TCP) 세그먼트의 제어 플래그인 'FIN', 보겨스(Bogus), 분할 옵션(fragmentation option) 비트, 전송제어프로토콜(TCP) 세그먼트의 윈도우 크기(Window Size) 비트, 전송제어프로토콜(TCP) 세그먼트의 옵션들(Options), 승인값(ACK Value), 인터넷제어메시지프로토콜(ICMP : Internet Control Message Protocol) 에러 등을 대상 서버에 보내면 핑거프린트(FingerPrint)로 간주한다. 여기서 인터넷제어메시지프로토콜(ICMP)의 메시지는 인터넷프로토콜(IP) 데이터그램의 데이터 필드에 포함된다.

조치방법 : 핑거프린트(FingerPrint)로 탐지되면 공격자가 예상하지 못하는 패킷을 보내어 운영체계(OS)를 파악하지 못하도록 한다.

-제7패턴-

공격명 : 사용자 데이터그램 프로토콜 플러딩(UDP Flooding)

공격방법 : 도스(DOS)공격의 한 방법으로서 사용자 데이터그램 프로토콜(UDP ; User Datagram Protocol)을 이용하여 공격자가 대상 서버에 가상의 데이터를 연속적으로 보내어 대상 서버의 부하를 발생시켜 정상적인 서비스를 하지 못하도록 한다.

탐지방법 : 공격자가 사용자 데이터그램 프로토콜(UDP)을 이용하여 동일 데이터를 반복적으로 대상 서버에 보낼 경우 사용자 데이터그램 프로토콜 플러딩(UDP Flooding)으로 간주한다.

조치방법 : 사용자 데이터그램 프로토콜 플러딩(UDP Flooding) 정보를 본 발명의 원격 중앙 관리자인 클라이언트에게 알리고, 그 클라이언트는 불필요한 사용자 데이터그램 프로토콜(UDP) 서비스를 디스에이블(Disable)시킴으로서 공격의 피해를 최소화한다.

-제8패턴-

공격명 : 사용자 데이터그램 프로토콜 포트 스캔(UDP Port Scan)

공격방법 : 해킹을 위해 대상 서버(컴퓨터)가 사용자 데이터그램 프로토콜(UDP)의 어떤 포트를 오픈(open)하여 서비스하고 있는지 알아내어 공격하는 방법으로, 그 포트번호 0번부터 65,535번까지의 포트에 순차적 또는 무순위로 데이터를 보내어 대상 서버가 인터넷제어메시지프로토콜(ICMP)로 응답하는 것을 확인한다.

탐지방법 : 특정 공격자(해커)가 특정 대상 서버에게 포트를 달리하여 보내는 사용자 데이터그램 프로토콜(UDP) 데이터의 개수를 계산하여, 일정량 이상의 사용자 데이터그램 프로토콜(UDP)을 보내는 것으로 판단되면 포트 스캔(Port Scan)으로 분류한다.

조치방법 : 본 발명의 네트워크 보호 서버인 스나이퍼는 원격 중앙 관리자인 클라이언트에게 포트 스캔 발생 사실을 알리고, 그에 따라 클라이언트는 대상 서버의 불필요한 사용자 데이터그램 프로토콜(UDP)의 서비스 포트를 디스에이블(Disable)시킨다. 그로써 해킹 공격을 최소화한다.

-제9패턴-

공격명 : 인터넷제어메시지프로토콜 스매프(ICMP Smuf)

공격방법 : 공격자가 대상 서버를 마비시키기 위해서 제3의 시스템들에게 에코 명령어(ECHO)를 보낼 때 응답지인 대상 서버로 패킷을 변조하여 보내는 방법이다. 이로 인해 대상 서버 및 네트워크의 부하량이 증가하여 대상 서버가 정상적으로 서비스하지 못하게 된다.

탐지방법 : 인터넷제어메시지프로토콜(ICMP) 응답 패수가 대량으로 발생하면 인터넷제어메시지프로토콜 스마프(ICMP Smurf)로 간주한다.

조치방법 : 공격 정보를 네트워크 또는 시스템 관리자에게 알림으로서 원격 중앙 관리자가 방화벽(Firewall)에서 인터넷제어메시지프로토콜(ICMP) 서비스(즉 ECHO 서비스)를 차단하여 해결한다.

-제10패턴-

공격명 : 핑 플러딩(Ping Flooding)

공격방법 : 해커는 네트워크가 정상적으로 작동하는지 여부를 확인하기 위해 사용되는 핑테스트(Ping Test)를 해킹 대상 서버(컴퓨터)를 확인하기 위한 방법으로 사용한다.

탐지방법 : 특정 공격자가 특정 대상 서버에 30회 이상 핑 명령어(Ping)를 보낼 경우에 이를 핑 플러딩(Ping Flooding)으로 간주한다.

조치방법 : 공격 정보를 네트워크 또는 시스템 관리자에게 알림으로서 원격 중앙 관리자가 방화벽(Firewall)에서 그 공격을 차단하거나, 그 해킹 공격을 가하는 공격지를 집중적으로 관찰한다.

-제11패턴-

공격명 : 트레이스 루트(Trace Route)

공격방법 : 공격자(해커)가 네트워크 경로를 사전에 파악하기 위해 사용한다.

탐지방법 : 인터넷프로토콜(IP) 데이터그램의 시간 지정(Time of live) 필드값을 '0'으로 하여 인터넷제어메시지프로토콜(ICMP)의 개수를 파악하여 탐지한다.

조치방법 : 그 공격 정보를 원격 중앙 관리자인 클라이언트에게 주지시켜 집중적으로 관찰하도록 한다.

-제12패턴-

공격명 : 메일 폭탄(Mail Bomb)

공격방법 : 메일 서버에 대량의 이메일(e-mail)을 보내어 메일 서버의 용량을 초과하게 만듦으로서 메일 서버의 고유 기능을 마비시킨다.

탐지방법 : 대량의 이메일을 보내기 위해서는 수작업으로는 불가능하기 때문에 프로그램을 이용하여 동일한 내용(반드시 동일하지 않을 수도 있지만 대부분 유사한 방식으로 구성되어 있음)의 이메일을 특정 공격자가 메일 서버에 전달하는 공격이다. 본 발명의 네트워크 보호 서버인 스니퍼는 이 공격을 감시하며 탐지한다.

조치방법 : 동일하거나 유사한 이메일이 3회 이상 특정 대상 서버에게 전달될 경우, 스니퍼가 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 리셋(RESET) 신호를 공격자와 대상 메일 서버에 동시에 보냄으로서 더 이상의 이메일이 그 대상 메일 서버에 전달되지 못하게 함으로써 그 대상 메일 서버를 보호한다.

-제13패턴-

공격명 : 메일의 사용자 확인(Mail Verify User)

공격방법 : 이메일(e-mail)을 주고받기 위해서는 서버에 반드시 메일 프로그램이 실행되어 있어야 한다. 이러한 점을 이용하여 대상 메일 서버에 어떤 사용자가 있는지에 대한 정보를 파악한다.

탐지방법 : 공격자가 입력하는 메일의 사용자 확인(Mail Verify User)을 감시하여 2회 이상 그에 해당 명령어가 감지되면 사용자 정보를 파악하기 위한 공격으로 간주한다.

조치방법 : 공격자와 그 대상 메일 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 그 대상 메일 서버의 사용자 정보를 보호한다.

-제14패턴-

공격명 : 메일 No Op 플러딩(Mail No Op Flooding)

공격방법 : 메일 서버에 명령어 'Mail No Op'를 다량으로 보내어 서버를 다음(down)시키거나, 예상하지 못한 일을 하게 함으로서 공격이 이루어진다.

탐지방법 : 공격자와 그 대상 서버가 주고받는 명령어를 감시하여 명령어 'Mail No Op'를 대상 서버에 반복해서 보내면 그 공격으로 간주한다.

조치방법 : 공격자와 그 대상 메일 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 그 대상

메일 서버를 보호한다.

-제15패턴-

공격명 : 메일 불량 명령어(Mail Bad Command)

공격방법 : 이메일을 주고받기 위해서는 미리 정해진 규약(SMTP : Simple Mail Transfer Protocol)을 반드시 이용하여야 하는데, 공격자가 임의로 그 규약을 어기고 이상한 명령어를 대상 서버에 보냄으로써, 그 대상 서버를 다운(down)시키거나 예상하지 못한 일을 하게 함으로서 공격이 이루어진다.

탐지방법 : 공격자와 대상 서버가 주고받는 명령어를 감시하여 정해진 규약(SMTP)에 어긋나는 명령어가 탐지되면 공격으로 간주한다.

조치방법 : 공격자와 그 대상 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로써 그 대상 서버를 보호한다.

-제16패턴-

공격명 : 파일전송프로토콜 포트 바운드(FTP Port Bound)

공격방법 : 해킹을 위해 대상 서버(컴퓨터)가 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 어떤 포트를 오픈(Open)하여 서비스를 하고 있는지 알아내어 공격하는 방법으로, 그 포트번호를 파일전송프로토콜(FTP) 데이터가 기본적으로 사용하는 1024번 이상의 포트 대신에 1024번 아래의 포트를 오픈(Open)하여 대상 서버의 서비스 포트를 알아내는 방법이다.

탐지방법 : 파일전송프로토콜(FTP) 데이터 패킷이 1024번 아래의 포트를 오픈(Open)하면 파일전송프로토콜 포트 바운드(FTP Port Bound) 공격으로 간주한다.

조치방법 : 공격자와 대상 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 대상 서버를 보호한다.

-제17패턴-

공격명 : 파일전송프로토콜 위반(FTP Violation)

공격방법 : 익명(Anonymous)으로 파일전송프로토콜(FTP) 서비스를 할 경우에, 공격자가 접속 후 그 대상 서버의 환경설정을 파악하여 허용 권한 이상의 행동을 함으로써 정보를 파괴하거나 획득하는 공격 방법이다.

탐지방법 : 익명의 파일전송프로토콜(Anonymous FTP) 서버에 접속한 공격자가 권한 밖의 명령어(Write, Delete 등)를 실행하는 것을 감지하여 파악한다.

조치방법 : 공격자와 대상 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 그 대상 서버를 보호한다.

-제18패턴-

공격명 : 승인 스톰(Ack Storm)

공격방법 : 공격자가 특정 대상 서버에 하이잭킹(Hi-jacking) 공격을 하기 위한 방법으로, 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 패킷 번호를 알아내기 위해서 반복적으로 특정 대상 서버에 승인(ACK) 신호를 보낸다.

탐지방법 : 공격자가 보내는 승인(ACK) 신호 개수를 파악하여 일정 비율 이상을 차지할 경우 승인 스톰(ACK Storm)으로 간주한다.

조치방법 : 공격자와 대상 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 대상 서버를 보호한다.

-제19패턴-

공격명 : 버퍼 오버플로우(Buffer Overflow)

공격방법 : 특정 대상 서버가 서비스하는 웹 서비스(Web service), 텔넷 서비스(Telnet), 파일전송프로토콜 서비스(FTP), Rlogin 서비스, 단순메일전송프로토콜(SMTP) 서비스 등의 프로그램에 예상하지 못한 수 많은 문자열을 보냄으로서 대상 서버를 다운시키거나 예상치 못한 일을 하게 함으로서 공격이 이루어진다.

탐지방법 : 웹 서비스(Web service), 텔넷 서비스(Telnet), 파일전송프로토콜 서비스(FTP), Rlogin 서비스, 단순메일전송프로토콜(SMTP) 서비스 등의 프로그램에서 처리할 수 있는 문자열 보다 많은 문자열이 대상 서버로 보내질 때 이를 버퍼 오버플로우(buffer overflow) 공격으로 간주한다.

조치방법 : 공격자와 대상 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 대상 서버를 보호한다.

-제20패턴-

공격명 : 로긴 실패(Login Fail)

공격방법 : 해커가 대상 서버에 텔넷 서비스(Telnet), 파일전송프로토콜 서비스(FTP), Rlogin 서비스 등을 이용하여 대상 서버에 접속함으로써, 그 대상 서버의 기능을 마비시키거나 그 대상 서버로부터 정보를 획득 또는 훼손시킨다.

탐지방법 : 텔넷 서비스(Telnet), 파일전송프로토콜 서비스(FTP), Rlogin 서비스 등을 이용하여 대상 서버에 접근하기 위해서는 반드시 식별자(ID)와 패스워드(PASSWORD)가 있어야 하지만, 해커는 추측으로 식별자(ID)와 패스워드(PASSWORD)를 입력한다는 점에 착안하여 연속해서 3회 이상 로긴(Login)에 실패할 경우 이를 집중 관리 대상자로 분류한다.

조치방법 : 연속 3회 이상 로긴(Login)에 실패한 사용자를 1시간 이내에는 그 대상 서버에 접속하지 못하도록 함으로서 대상 서버를 보호한다.

-제21패턴-

공격명 : 인터넷프로토콜 스푸핑(IP Spoofing)

공격방법 : 대상 서버가 동일한 랜(LAN) 환경 또는 넷마스크(Netmask)를 가진 사용자에게는 다양한 서비스를 제공하고, 그렇지 않은 사용자에게는 서비스를 제한하도록 설계되어 있을 경우에, 해커가 외부 네트워크에서 대상 서버에 침투할 때 마치 내부 네트워크 사용자인 것처럼 인터넷프로토콜(IP) 주소를 속여서 대상 서버에 접근한다.

탐지방법 : 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 패킷에는 인터넷프로토콜 주소(IP Address)와 네트워크 하드웨어의 주소(MAC Address)가 항상 포함된다는 점을 이용하여, 항상 미리 기록된 라우터의 하드웨어 주소(MAC Address)와 전송제어프로토콜/인터넷프로토콜(TCP/IP)의 하드웨어 주소(MAC Address)를 비교함으로서 탐지한다.

조치방법 : 공격자와 대상 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 대상 서버를 보호한다.

-제22패턴-

공격명 : 티어드롭(Tear Drop)

공격방법 : 송신측에서는 인터넷프로토콜(IP) 데이터그램을 분할(fragmentation)하고, 수신측에서는 이를 조합(reassembly)하는 매우 정상적인 과정을 교묘하게 함으로서 대상 서버(컴퓨터)를 다운(down)시키는 도스(DOS)공격의 일종이다. 윈도우즈 95와 윈도우즈 엔티(Windows NT)가 주공격 대상이지만, 리눅스(LINUX)의 경우 커널 2.0이나 커널 32 이전의 버전이 주공격 대상이다.

탐지방법 : 전송제어프로토콜/인터넷프로토콜(TCP/IP) 패킷이 오버랩핑(Overlapping)되어 있거나, 인터넷프로토콜(IP) 데이터그램이 매우 작게 조개져 있을 경우 티어드롭(Tear Drop)으로 간주한다.

조치방법 : 1. 이러한 공격 정보를 원격 중앙 관리자에게 주지시켜 집중적으로 관찰하도록 한다.

2. 해당하는 대상 서버의 운영체계(OS) 버전을 높여서 공격의 피해를 최소화한다.

-제23패턴-

공격명 : 호스트 스위핑(Host Sweeping)

공격방법 : 각종 정보를 파악할 수 있는 기법(FingerPrint, Ping, Port Scan 등)을 동원하여 각종 대상 서버의 정보를 파악하는 공격 방법이다.

탐지방법 : 한 공격자가 여러 대상 서버를 순차적으로 스캔(Scan) 할 경우 호스트 스위핑(Host Sweeping)으로 간주한다.

조치방법 : 이러한 공격 정보를 원격 중앙 관리자에게 주지시켜 집중적으로 관찰하도록 한다.

-제24패턴-

공격명 : 윈도우즈 누크(Windows Nuke)

공격방법 : 전송제어프로토콜(TCP)이 오오비 대역외(OOB-out of band) 데이터를 처리할 때 사용하는 'URG' 신호를 윈도우즈(Windows)의 139 포트(NetBios over TCP)에 보냄으로서, 대상 서버를 다운시키거나 비정상적인 사용자를 정상적인 사용자로 오인하게 만드는 공격 방법이다.

탐지방법 : 넷바이어스 포트(NetBios Port) 139 포트에 'URG' 신호를 보내는 것을 감시하여 탐지한다.

조치방법 : 1. 공격자와 대상 서버에 리셋(RESET) 신호를 보내어 공격을 무력화시킴으로서 대상 서버를 보호한

2. 대상 서버의 운영체계(OS) 버전을 높여서 공격의 피해를 최소화한다.

-제25패턴-

공격명 : 랜드공격(Land Attack)

공격방법 : 공격자가 임의로 자신의 인터넷프로토콜 주소(IP Address) 및 포트를 대상 서버의 인터넷프로토콜 주소(IP Address) 및 포트와 동일하게 하여 그 대상 서버에 접속함으로서, 그 대상 서버의 실행 속도를 느려지게 하거나 실행을 마비시킨다.

탐지방법 : 공격지와 대상 서버의 각 인터넷프로토콜 주소(IP Address)와 각 포트가 동일한지 여부를 확인한다.

조치방법 : 이러한 공격 정보를 원격 중앙 관리자에게 주지시켜 집중적으로 관찰하도록 한다.

-제26패턴-

공격명 : 인터넷프로토콜 충돌(IP Collision)

공격방법 : 인터넷프로토콜 주소(IP Address)를 이미 사용하고 있는 인터넷프로토콜 주소(IP Address)로 설정함으로서 기존에 사용되고 있던 대상 서버의 네트워크를 다운시키는 공격 방법이다. 이는 반드시 공격이라고는 단정할 수는 없다.

탐지방법 : 본 발명의 네트워크 보호 서버인 스니퍼에 각각의 시스템에 설치되어 있는 랜카드(Lancard)의 유일 하드웨어 주소(Mac Address)와 인터넷프로토콜 주소(IP Address)를 테이블화하여 스니퍼에 구축한 다음 특정 시스템이 중복된 인터넷프로토콜 주소(IP Address)를 설정하면 자동으로 탐지된다.

조치방법 : 중복된 내용을 원격 중앙 관리자에게 알려서 수정되도록 한다.

-제27패턴-

공격명 : 핑거(Finger)

공격방법 : 해커가 어떤 시스템에 어떤 사용자가 존재하는지에 대한 확인 방법으로 사용하는 핑거(Finger) 프로토콜을 해킹을 위한 정보로 활용한다.

탐지방법 : 외부 네트워크에서 내부 네트워크의 대상 서버로 핑거 명령어(Finger)가 들어오면, 이를 탐지한다. (본 발명의 스니퍼에서는 내부 사용자가 내부 네트워크의 대상 서버에 핑거 명령어(Finger)를 보내는 것을 허용한다)

조치방법 : 공격자와 대상 서버에 리셋(RESET)신호를 보내어 그 해커가 정보를 획득하지 못하도록 한다.

-제28패턴-

공격명 : 웹을 이용한 정보 획득

공격방법 : 웹 서버의 버그(Bug) 및 백도어(Back door)를 이용한 정보 획득 공격으로서, 웹 브라우저(Web Browser)의 유알엘(URL) 입력 부분에 각종 패턴을 입력한다. 또한 유알엘(URL)에 대량의 문자열을 입력하여 대상 서버에 버퍼 오버플로우(Buffer Overflow)가 발생되도록 하여 공격한다.

탐지방법 : 상기의 제1패턴에서 제27패턴을 포함하여 현재까지 알려진 해킹 패턴을 비교하여 탐지한다.

조치방법 : 1. 공격자와 대상 서버에 리셋(RESET) 신호를 보내어 해커가 정보를 획득하지 못하도록 한다.

2. 원격 중앙 관리자는 버그(Bug)와 수정된 웹 서버로 버전을 높인다.

상기 설명된 각 해킹 패턴을 탐지하고 그에 따른 조치 방법을 제공하는 본 발명의 네트워크 보호 시스템은 네트워크 사용자수에 따라 네트워크 보호 서버의 하드웨어 사양을 달리하여 적용할 수 있는데, 메인 메모리(ECC SDRAM)와 하드디스크(HDD)의 용량만을 교체하여 실현할 수 있다.

발명의 효과

이상에서 설명한 바와 같이 본 발명의 네트워크 보호 시스템은 외부로부터 들어오는 복잡하고 다양한 침입 패턴의 해킹(특히 크래킹)과 같은 불법적인 침입 행위를 자동으로 탐지하고 차단함은 물론 그 근원지를 추적하여 정확한 해킹 증거를 제공할 수 있기 때문에, 보다 근본적인 보안 체계를 구축하는데 효과적이다.

또한 본 발명의 네트워크 보호 시스템은 패킷 필터링 방식을 사용하므로 내부 네트워크에 대한 부하 영향이 최소화되며, 네트워크 보호를 위한 소프트웨어와 하드웨어가 일체형이기 때문에 네트워크 보호 장비(스니퍼)의 설치와 사용이 용이하다.

특히 본 발명의 네트워크 보호 시스템은 네트워크 사용자수에 따라 네트워크 보호 서버의 하드웨어 사양을 달리하여 적용할 수 있다. 따라서 사용자수가 100인 미만인 소용량의 네트워크를 사용하는 중소 기업

체 및 일반 관공서와, 사용자수가 300인 미만인 중용량의 네트워크를 사용하는 기업체 및 관공서와, 사용자수가 300인 이상인 대용량의 네트워크를 사용하는 대기업체 및 관공서에 모두 적용된다.

(또) 청구의 범위

청구항 1

각각 독립된 내부 네트워크와 외부 네트워크를 최적의 경로로 상호 연결시키는 라우터와,

상기 라우터에 의해 상호 연결된 경로를 통한 통신에 대해 일차적으로 감시하고 통제하는 방화벽과,

상기 방화벽에서 허가한 통신에 대해 실시간으로 감시하면서 비인가/비정상적인 통신을 구별 탐지하고, 그 탐지 내역으로부터 해당 네트워크 세션을 전략적으로 차단하고, 그 탐지 내역을 시각적 청각적으로 보고하고, 그 탐지 내역에 대한 정보를 관리하는 네트워크 보호 서버를 포함하여 구성되는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 2

제 1 항에 있어서, 웹 인터페이스를 통해 상기 네트워크 보호 서버에서 제공되는 네트워크 보호 어플리케이션을 원격지의 관리자가 실행시키기 위한 클라이언트 컴퓨터가 더 구비되는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 3

제 2 항에 있어서, 상기 원격지 관리자는 상기 네트워크 보호 서버에 의해 실시간으로 감시되고 있는 현재 통신에서 원격지의 사용자 명령어를 상기 클라이언트 컴퓨터를 통해 온라인(on-line)으로 검색하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 4

제 1 항에 있어서, 상기 네트워크 보호 서버는

상기 내부 네트워크 대에서의 통신과, 상기 내부 네트워크와 상기 외부 네트워크간의 통신을 실시간으로 감시하기 위한 네트워크 감시 수단과,

상기 네트워크 감시 수단을 통해 감시되는 통신 중에서 상기 비인가/비정상적인 통신을 구별하고 탐지하기 위한 네트워크 탐지 수단과,

상기 네트워크 탐지 수단에 의해 탐지된 상기 비인가/비정상적인 통신을 차단하기 위한 접근 차단 수단과,

상기 네트워크 탐지 수단에 의한 비인가/비정상적 통신의 탐지 사실을 원격지의 관리자에게 유선 또는 무선으로 알리기 위한 경보 수단과,

상기 네트워크 탐지 수단에 의해 탐지된 그 탐지 내역의 보고서를 상기 원격지의 관리자에게 제공하기 위한 감시내역 보고 수단으로 구성되는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 5

제 4 항에 있어서, 상기 네트워크 감시 수단은, 미리 정해진 옵션에 따라 상기 내부 네트워크 내에서의 통신과, 상기 내부 네트워크와 상기 외부 네트워크간의 통신을 정해진 시간대별로 감시하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 6

제 4 항에 있어서, 상기 네트워크 감지 수단은, 원격지의 상기 외부 네트워크로부터 접근하는 통신에서 사용자 명령어를 감시하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 7

제 4 항에 있어서, 상기 네트워크 감시 수단은 상기 네트워크 탐지 수단과 연계되어 동작하며, 통신되는 네트워크 데이터를 스캔(scan)하고 캡쳐(capture)하는 수동방식으로 감시하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 8

제 4 항에 있어서, 상기 네트워크 감시 수단은 상기 네트워크 탐지 수단과 연계하여 상기 내부 네트워크에서 임의의 외부 네트워크로 발송되는 이메일(전자우편)에 대한 키워드 검색 및/또는 로깅을 실시하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 9

제 8 항에 있어서, 상기 네트워크 감시 수단은 상기 네트워크 탐지 수단과 연계하여 상기 발송되는 이메일의 발송자와 접수자에 대한 정보를 감시하고, 상기 발송되는 이메일의 내용(본문과 첨부파일)을 검열하여 상기 내부 네트워크에서 정한 특정 문자열이 탐지되는 지를 감시하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 10

제 9 항에 있어서, 상기 네트워크 감시 수단 및 상기 네트워크 탐지 수단에 의해 상기 특정 문자열이 탐

지될 경우, 상기 접근 차단 수단은 그 해당 이메일의 발송을 차단하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 11

제 4 항에 있어서, 상기 네트워크 탐지 수단은, 상기 네트워크 감시 수단을 통해 감시되는 통신 중에서 미리 알려진 다수의 해킹 패턴을 구별하고 탐지하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 12

제 4 항에 있어서, 상기 네트워크 탐지 수단은, 상기 네트워크 통신을 통해 수신되는 인터넷프로토콜(IP) 데이터그램의 헤더에 삽입되는 유효한(on) 제어 플래그와 그 제어 플래그에 대한 승인(ACK) 개수를 계산하여, 미리 정해진 개수 이상의 과도 발생 여부를 탐지하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 13

제 12 항에 있어서, 상기 네트워크 탐지 수단에 의해 과도 발생이 탐지된 경우에, 상기 접근 차단 수단은 상기 제어 플래그 발송측과 그 제어 플래그 수신측에 상기 계산된 개수에 상응하는 개수의 리셋(RESET) 신호를 보내는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 14

제 4 항에 있어서, 상기 네트워크 탐지 수단은, 상기 네트워크 통신을 통해 수신되는 전송제어프로토콜/인터넷프로토콜(TCP/IP) 패킷의 헤더에 삽입되는 유효한(on) 제어 플래그가 상기 제어 플래그 수신측의 포트를 달리하여 일정량 이상 접근하는지의 여부를 탐지하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 15

제 14 항에 있어서, 상기 수신측의 포트를 달리한 일정량 이상의 접근이 상기 네트워크 탐지 수단에 의해 탐지된 경우에, 상기 접근 차단 수단은 상기 제어 플래그 수신측의 불필요한 포트를 디스에이블(Disable) 시키는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 16

제 4 항에 있어서, 상기 경보 수단은, 상기 네트워크 탐지 수단에 의해 비인가/비정상적 통신이 탐지될 경우에 무선통신망의 문자메시지 서비스를 이용하여 그 탐지 사실 및 탐지 내용을 원격지 관리자의 무선 통신단말기로 전송하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 17

제 4 항에 있어서, 상기 경보 수단은, 상기 네트워크 탐지 수단에 의해 비인가/비정상적 통신이 탐지될 경우에 무선통신망의 음성메시지 서비스를 이용하여 그 탐지 사실 및 탐지 내용을 원격지 관리자의 무선 통신단말기로 전송하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 18

제 1 항에 있어서, 상기 네트워크 보호 서버의 구동 및 운영을 위한 운영체계로써 리눅스(LINUX)가 사용되는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 19

제 1 항에 있어서, 상기 네트워크 보호 서버는 상기 방화벽을 통해 상기 라우터와 접속되는 다수의 허브(HUB)에 연결되며, 상기 허브는 상기 내부 네트워크의 다수의 서버 및 다수의 컴퓨터들을 집선함과 동시에 또다른 네트워크 내부의 다수 서버 및 다수 컴퓨터들을 집선하는 임의의 또다른 허브와 연결되는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 20

특정 내부 네트워크 내에서의 통신과, 상기 내부 네트워크와 상기 외부 네트워크간의 통신을 실시간으로 감시하기 위한 네트워크 감시 엔진과, 상기 네트워크 감시 엔진을 통해 감시되는 통신 중에서 특정 해킹 패턴을 구별하고 탐지하기 위한 네트워크 탐지 엔진과, 상기 네트워크 탐지 엔진에 의해 탐지된 해킹을 차단하기 위한 접근 차단 엔진과, 상기 네트워크 탐지 엔진에 의한 해킹 탐지 사실을 원격지의 관리자에게 유선 또는 무선으로 알리기 위한 경보 엔진과, 상기 네트워크 탐지 엔진에 의해 탐지된 그 탐지 내역의 보고서를 상기 원격지의 관리자에게 제공하기 위한 감시내역 보고 엔진을 포함하는 네트워크 보호 서버와;

상기 네트워크 보호 서버의 상기 각 엔진들의 실행을 위한 웹 사이트를 웹 인터페이스 시켜주는 웹 서버로 구성되어, 상기 네트워크 보호 서버 및 상기 웹 서버의 구동 및 운영을 위한 운영체계로써 리눅스(LINUX)가 장착되어 사용되는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 21

제 20 항에 있어서, 상기 웹 인터페이스에 의한 상기 웹 사이트로의 접속을 지원하는 웹 브라우저를 내장하며, 상기 네트워크 보호 서버의 각 엔진들에 의한 어플리케이션을 실행하기 위한 사용자 인터페이스를 제공하는 상기 원격지 관리자의 컴퓨터가 더 구비되는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 22

제 20 항에 있어서, 상기 네트워크 보호 서버는, 상기 내부 네트워크와 상기 외부 네트워크간의 통신을 통해 송수신되는 전송제어프로토콜(TCP) 세그먼트(segment)의 헤더(header)를 분석하고 또한 인터넷프로

토콜(IP) 데이터그램(datagram)의 헤더(header)를 분석하여 상기 외부 네트워크로부터 접근하는 사용자 명령어를 실시간 감시하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 23

제 22 항에 있어서, 상기 네트워크 보호 서버는 상기 헤더들의 분석을 통해 상기 외부 네트워크로부터의 해킹 침입 경로를 라우터 단위로 추적하고, 그에 따른 해킹 증거를 웹 인터페이스를 통해 상기 원격지 관리자에게 제공하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 24

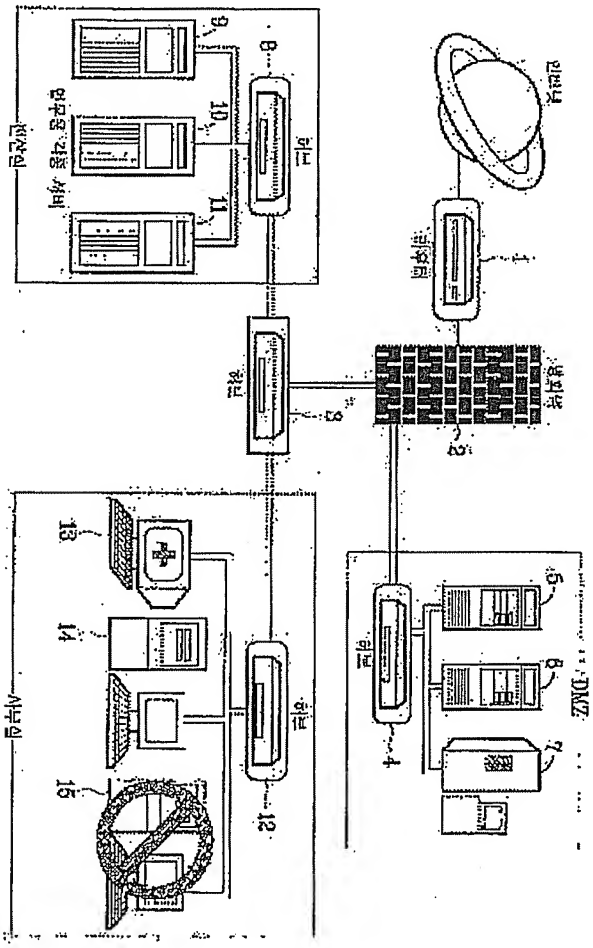
제 23 항에 있어서, 상기 네트워크 보호 서버는 상기 해킹 침입 경로 추적을 통한 해킹 근원지 탐지를 위해 인터넷의 도메인 네임 시스템(DNS) 정보를 관리하는 공식적 센터와 연결되며, 상기 공식적 센터에 상기 외부 네트워크로부터 접근하는 외부사용자 및 외부서버의 정보를 의뢰하는 것을 특징으로 하는 네트워크 보호 시스템.

청구항 25

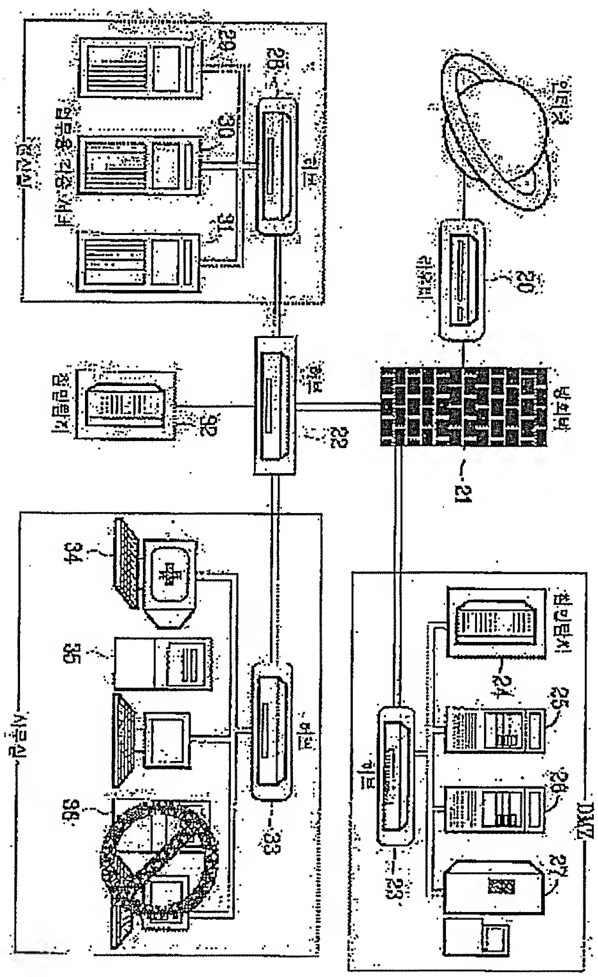
제 24 항에 있어서, 상기 네트워크 보호 서버는, 상기 공식적 센터에 상기 해킹 근원지 정보를 의뢰하고, 상기 공식적 센터로부터 제공받은 해킹 근원지 정보를 토대로 캐쉬 테이블(Cache table)을 구축하는 것을 특징으로 하는 네트워크 보호 시스템.

도면

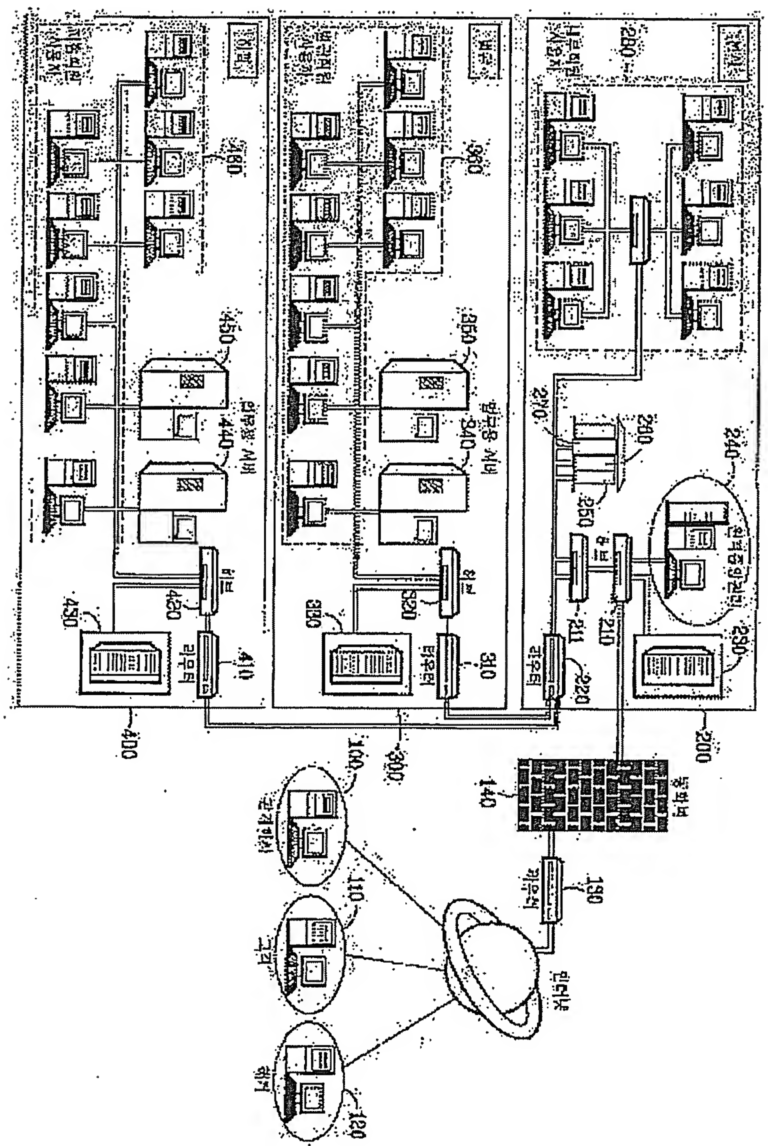
도면1



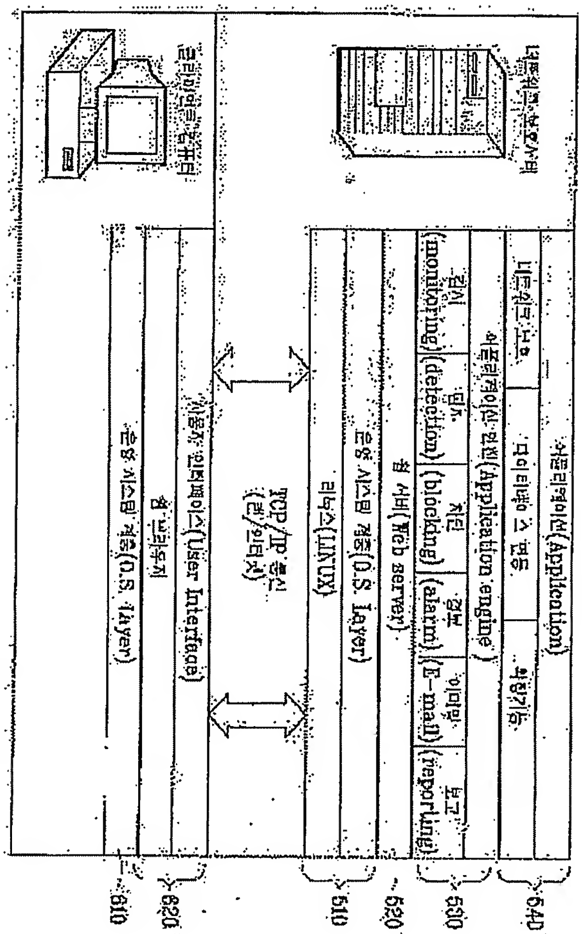
도면2



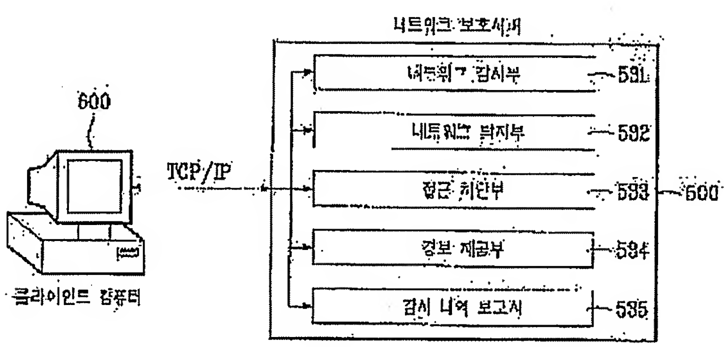
도면3


400
300
200
410
420
430
440
450
460
310
320
330
340
350
360
210
211
220
230
240
250
260
270
280
140
130
160
110
120

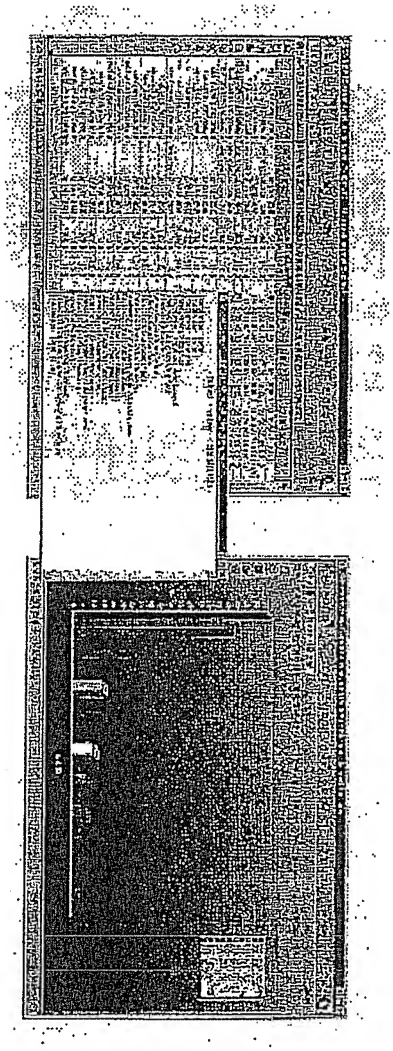
도면4


클라이언트 컴퓨터
네트워크 보호서버
운용 시스템 계층(O.S. layer)
웹 브라우저
사용자 인터페이스(User Interface)
TCP/IP 통신
(랜/인터넷)
리눅스(LINUX)
운용 시스템 계층(O.S. layer)
웹 서버(Web server)
애플리케이션 엔진(Application engine)
감시 (monitoring)
탐지 (detection)
차단 (blocking)
경보 (alarm)
이메일 (E-mail)
보고 (reporting)
네트워크 노드
데이터베이스 관리
부가기능
애플리케이션(Application)
610
620
510
520
530
540

도면5

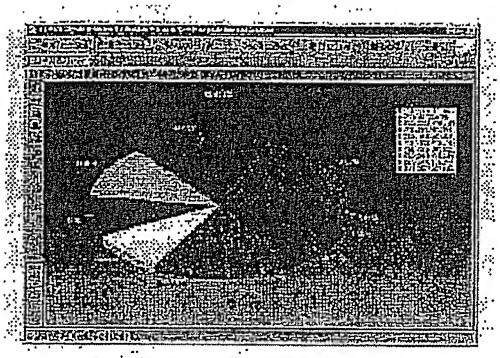

600
클라이언트 컴퓨터
TCP/IP
네트워크 보호서버
네트워크 감시부
591
네트워크 탐지부
592
접근 차단부
593
경보 제공부
594
감시 내역 보고서
595
600

도면6

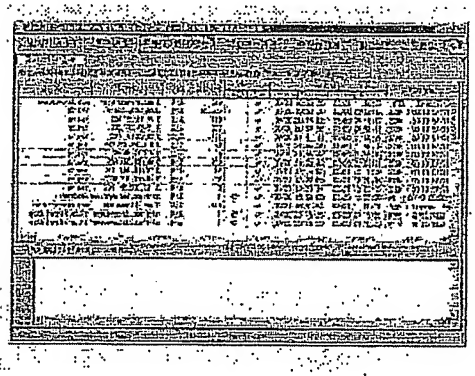


도면7a

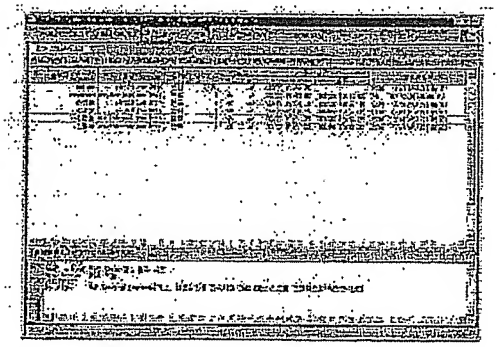
도면7b



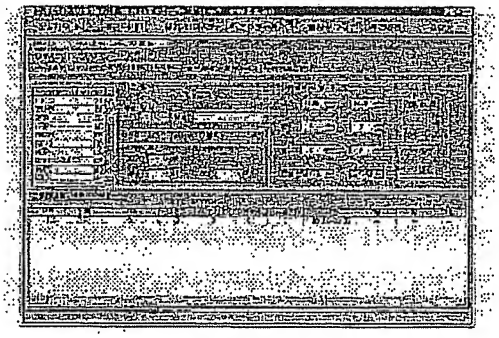
도면8a



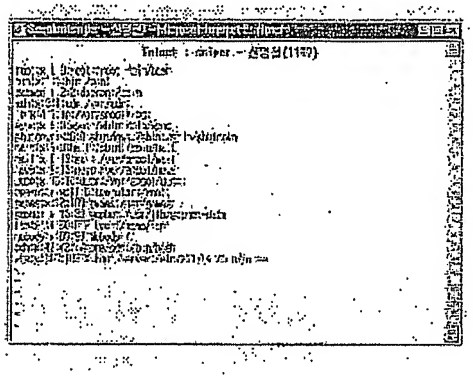
도면8b



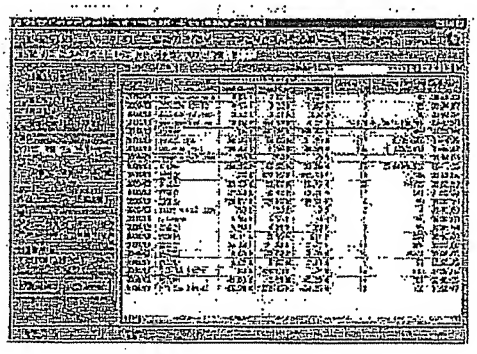
도면9



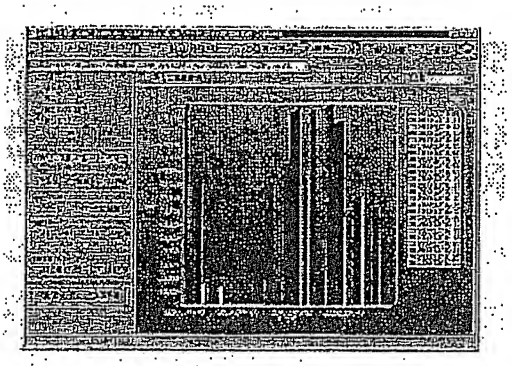
도면9a



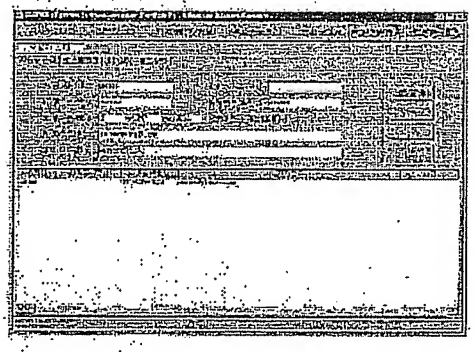
도면10



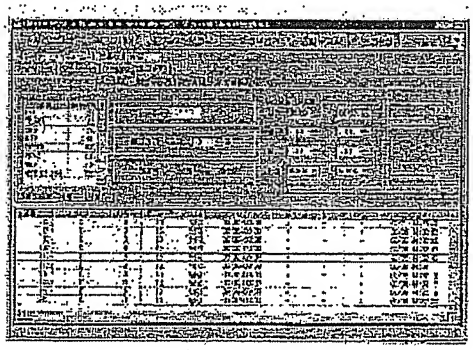
도면10b



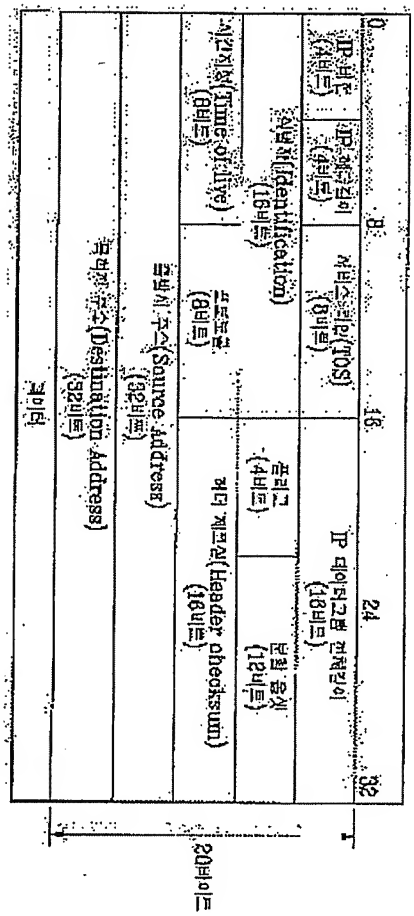
도면11a



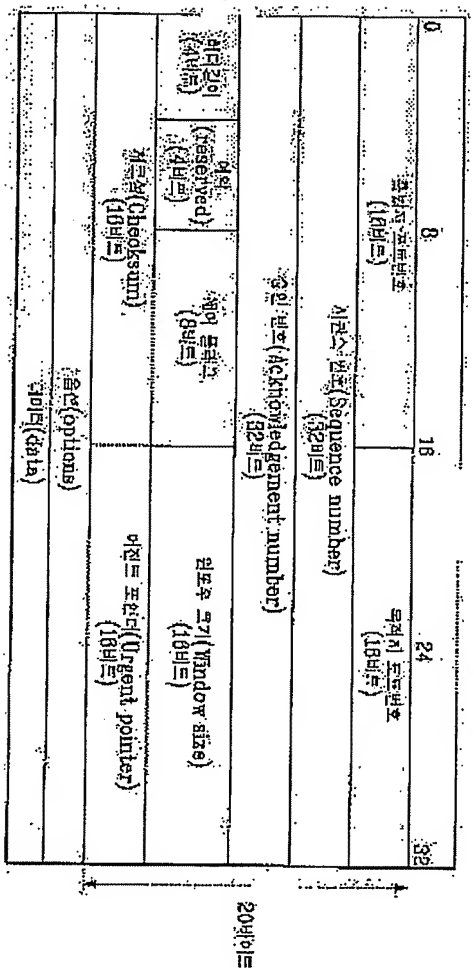
도면11b



도면12


0
8
16
24
32
IP 버전 (4비트)
IP 헤더길이 (4비트)
서비스형태(TOS) (8비트)
IP 데이터그램 길이 (16비트)
식별자(Identification) (16비트)
플래그 (4비트)
단편 옵셋 (12비트)
생존시간(Time of Live) (8비트)
프로토콜 (8비트)
헤더 체크섬(Header checksum) (16비트)
출발지 주소(Source Address) (32비트)
목적지 주소(Destination Address) (32비트)
데이터
20바이트

도면15


0
8
16
24
32
출발지 포트번호 (16비트)
목적지 포트번호 (16비트)
시퀀스 번호(Sequence number) (32비트)
승인 번호(Acknowledgement number) (32비트)
헤더 길이 (4비트)
Reserved (6비트)
윈도우 크기(Window size) (16비트)
체크섬(Checksum) (16비트)
긴급 포인터(Urgent pointer) (16비트)
옵션(options)
데이터(data)
20바이트